SJ Games vs. the Secret Service

On March 1 1990, the offices of Steve Jackson Games, in Austin, Texas, were raided by the U.S. Secret Service as part of a nationwide investigation of data piracy. The initial news stories simply reported that the Secret Service had raided a suspected ring of hackers. Gradually, the true story emerged.

More than three years later, a federal court awarded damages and attorneys' fees to the game company, ruling that the raid had been careless, illegal, and completely unjustified. Electronic civil-liberties advocates hailed the case as a landmark. It was the first step toward establishing that online speech IS speech, and entitled to Constitutional protection . . . and, specifically, that law-enforcement agents can't seize and hold a BBS with impunity.

The Raid

On the morning of March 1, without warning, a force of armed Secret Service agents - accompanied by Austin police and at least one civilian "expert" from the phone company - occupied the offices of Steve Jackson Games and began to search for computer equipment. The home of Loyd Blankenship, the writer of ***GURPS Cyberpunk***, was also raided. A large amount of equipment was seized, including four computers, two laser printers, some loose hard disks and a great deal of assorted hardware. One of the computers was the one running the Illuminati BBS.

The only computers taken were those with ***GURPS Cyberpunk*** files; other systems were left in place. In their diligent search for evidence, the agents also cut off locks, forced open footlockers, tore up dozens of boxes in the warehouse, and bent two of the office letter openers attempting to pick the lock on a file cabinet.

The next day, accompanied by an attorney, Steve Jackson visited the Austin offices of the Secret Service. He had been promised that he could make copies of the company's files. As it turned out, he was only allowed to copy a few files, and only from one system. Still missing were all the current text files and hard copy for this book, as well as the files for the Illuminati BBS with their extensive playtest comments.

In the course of that visit, it became clear that the investigating agents considered ***GURPS Cyberpunk*** to be "a handbook for computer crime." They seemed to make no distinction between a discussion of futuristic credit fraud, using equipment that doesn't exist, and modern real-life credit card abuse. A repeated comment by the agents was "This is real."

Over the next few weeks, the Secret Service repeatedly assured the SJ Games attorney that complete copies of the files would be returned "tomorrow." But these promises weren't kept; the book was reconstructed from old backups, playtest copies, notes and memories.

On March 26, almost four weeks after the raid, some (but not all) of the files were returned. It was June 21, nearly four *months* later, when most (but not all) of the hardware was returned. The Secret Service kept one company hard disk, all Loyd's personal equipment and files, the printouts of ***GURPS Cyberpunk,*** and several other things.

The raid, and especially the confiscation of the game manuscript, caused a catastrophic interruption of the company's business. SJ Games very nearly closed its doors. It survived only by laying off half its employees, and it was years before it could be said to have "recovered."

Why was SJ Games raided? That was a mystery until October 21, 1990, when the company finally received a copy of the Secret Service warrant affidavit - at their request, it had been *sealed.* And the answer was . . . guilt by remote association.

While reality-checking the book, Loyd Blankenship corresponded with a variety of people, from computer security experts to self-confessed computer crackers. From his home, he ran a *legal* BBS which discussed the "computer underground," and he knew many of its members. That was enough to put him on a federal List of Dangerous Hoodlums! The affidavit on which SJ Games were raided was unbelievably flimsy . . . Loyd Blankenship was suspect because he ran a technologically literate and politically irreverent BBS, because he wrote about hacking, and because he received and re-posted a copy of the */Phrack* newsletter. The company was raided simply because Loyd worked there and used its (entirely different) BBS!

As for ***GURPS Cyberpunk***, it had merely been a target of opportunity . . . something "suspicious" that the agents picked up at the scene. The Secret Service allowed SJ Games (and the public) to believe, for months, that the book had been the target of the raid.

The one bright spot in this whole affair was the creation of the Electronic Frontier Foundation. In mid-1990, Mitch Kapor, John Barlow and John Gilmore formed the EFF to address this and similar outrages. It's a nonprofit organization dedicated to preserving the Constitutional rights of computer users. (For more information, look at the EFF web site, or write them at 1550 Bryant Street, Suite 725, San Francisco, CA 94103-4832.) The EFF provided the financial backing that made it possible for SJ Games and four Illuminati users to file suit against the Secret Service.

Two active electronic-civil-liberties groups also formed in Texas: EFF-Austin and Electronic Frontiers Houston, which have since merged to become Electronic Frontiers Texas.

And science fiction writer Bruce Sterling turned his hand to journalism and wrote *The Hacker Crackdown* about this and other cases where the law collided with technology. A few months after it was published in hardback, he released it to the Net, and you can read it online.

In early 1993, the case finally came to trial. SJ Games was represented by the Austin firm of George, Donaldson & Ford. The lead counsel was Pete Kennedy.

And we won. The judge gave the Secret Service a tongue-lashing and ruled for SJ Games on two out of the three counts, and awarded over $50,000 in damages, plus over $250,000 in attorney's fees. In October 1994, the Fifth Circuit turned down SJ Games' appeal of the last (interception) count . . . meaning that right now, in the Fifth Circuit, it is not "interception" of your e-mail messages when law enforcement officials walk out the door with the computer holding them.

Case Documents

- The affidavit under which the Secret Service obtained its warrant to raid SJ Games. (This was first made public in issue 2.11 of the *Computer Underground Digest*, which we have reproduced here in its entirety to recognize the work of the CuD editors.)
- The complaint filed by SJ Games against the Secret Service.
- The final judge's decision in the case.
- The Fifth Circuit opinion on the "interception" question.

Articles and Commentary on Privacy, Search and Seizure, Etc.

- Bruce Sterling's Speech to the High Technology Crime Investigation Association (Lake Tahoe, November, 1994). Sterling tells the cops not to be pawns . . .
- Chilling Effect of BBS Raids on Electronic Speech. An example of self-censorship by a sysop group afraid of retaliation.
- Crime and Puzzlement (John Perry Barlow). The seminal article that launched the modern electronic civil liberties movement.
- CyberLaw Report on the SJ Games Case (Jonathan Rosenoer). The relevant issue of *CyberLaw*.
- Formulating A Company Policy on Access to and Use and Disclosure of Electronic Mail on Company Computer Systems (David R. Johnson and John Podesta)
- Practical Privacy Protection (Unless Congress Prohibits It) (Jim Warren). Electronic mail, cryptography and privacy.
- Press releases issued by SJ Games and the EFF after their victory in court.
- Steve Jackson Games v. U.S. Secret Service (Peter D. Kennedy). Analysis and discussion of the case, by one of the

attorneys who won it.

- The Constitution in Cyberspace (Laurence H. Tribe). A noted legal scholar calls for explicit Constitutional protection for electronic speech and writing.
- The Top Ten False Facts About The Secret Service Raid (Steve Jackson). A lot of things that the media "knows," that aren't so . . .
- The EFF's ten-year-later recap of the story.

Computer Law

- Texas Penal Code provisions regarding "computer crime." Updated 1994 . . .

Articles and Commentary on Censorship and Freedom of the Press

- Mike Godwin's speech against Usenet censorship at Carnegie-Mellon University.

Other Sources

- The Electronic Frontier Foundation
- Computer Underground Digest

Top of Page | Home

A Brief History of the Illuminati BBS

Illuminati Online hit the Internet in 1993. But its roots go back to the dawn of Austin BBSing. It was originally the Illuminati BBS, a customer-support board for Steve Jackson Games.

The Illuminati BBS officially went online on April 1, 1986. It ran on T-Net software (written in BASIC) on an Apple][+, with a screaming 300-baud modem. Our first hardware upgrade was a lower-case chip for the Apple . . .

The sysop was Fearless Leader. The actual identity of Fearless Leader was officially a secret. It wasn't Steve. Who was it? Good question.

The board's original purpose was game playtesting, discussion, and customer support. But soon it was clear that the Illuminati's online community was interested in much more than just games. Over the next few years, the user base grew to more than 1,000 - most of them paying long-distance rates to call - to discuss everything related to science fiction, fantasy, comics, gaming and general High Weirdness.

As the years went by and the Illuminati community grew, we upgraded both software and hardware. Our first changeover was to Joe-Net, a homebrew system written by local programmer Joe DiMaggio. Joe-Net was easy to use, full of features, and ran on a MS-DOS system, giving us a lot more speed. We loved it. But eventually, Joe didn't have the time to maintain the system. (He'd written it for fun, and in the history of the world as we know it there have only been three Joe-Net systems. Too bad. Best software we ever had.)

Fun with the Secret Service . . . Not!

Late in 1989, we switched to WWIV, a popular commercial software package which promised the capability to link to other BBSs nationwide. But that was not to be . . . On March 1, 1990, the SJ Games offices were raided by the Secret Service, in a now-famous "hacker hunt." They took the Illuminati computer (among other things) and loads of software, including our WWIV disks.

The old Apple][+ and T-Net were dragged out of the closet and pressed into service as an "answering machine" to tell callers what had happened - or as much as we knew. But Illuminati was down, and stayed down for a month.

We're Baaaaaaaaa-aaaack!

When we came back up, it was as a two-line system, on new hardware (some of it donated by our supporters). We were now running MCD-2, a locally written multiline package. We continued to use MCD-2 until 1993.

The system continued to grow, now with a strong added interest in civil liberties of computer users. When the search warrant was finally unsealed, it showed that the original raid had been a groundless fishing expedition, based on ignorance.

In 1992 we switched to an Amiga, running a multiline package called DLG. This gave us a lot more capabilities, but still wasn't enough . . . which was why we decided to go to the Internet and create this system.

Victory In Court

With the help of the newly-formed Electronic Frontier Foundation, SJ Games and several users filed suit and won substantial awards. In early 1993, a federal judge ruled that the Secret Service had to pay for the mail it had taken and read, the equipment it had damaged, and other harm to SJ Games.

And Now, The Internet

In August of 1993, the system added more than a dozen direct-dial lines and a T1 connection to the Internet, allowing for *hundreds* of simultaneous calls. Many new services were also added, including full Internet access for local callers and a vastly expanded conferencing system.

As of this writing (October 1998) we have more than 360 incoming lines in Austin, and a separate 48-line POP in Houston. We have 2 T1 lines, and a T3 to The Data Place, which has T3 connections to Sprint, MCI, AT&T and AlterNet, giving us a total of 48MB of bandwidth right out of out office. Illuminati Online has spun off as a separate company with its own offices on south IH-35 in Austin. We are adding more equipment constantly, and support over 7000 paying users.

Top of Page | Home

SECRET SERVICE SEARCH WARRANT AFFADAVIT

(COMPUTER UNDERGROUND DIGEST ISSUE 2.11)

This is the affidavit submitted by the Secret Service in order to get permission to raid the SJ Games offices on March First. Also included here is the relevant section of the Phoenix Project log - the material on which the Secret Service agent based his allegation of "conspiracy". [Note that the Secret Service did NOT append the actual log material to the affidavit the judge saw - but we're including it so YOU can see it. It's interesting that they chose to omit it. It's interesting that the magistrate granted the warrant anyway.]

The moderators of Computer Underground Digest re-typed all this material from a photocopy supplied by SJ Games. To acknowledge their effort, we are reproducing their issue 2.11 in the form they distributed it, complete with their editorial comments, rather than just publishing the affidavit itself.

Correspondence about CuD should go directly to its moderators.

  ****
                C O M P U T E R U N D E R G R O U N D
                          D I G E S T
            *** Volume 2, Issue #2.11 (November 13, 1990)   **
      *** SPECIAL ISSUE: SEARCH AFFIDAVIT FOR STEVE JACKSON GAMES ***
  ****

MODERATORS: Jim Thomas / Gordon Meyer (TK0JUT2@NIU.bitnet)
ARCHIVISTS: Bob Krause / Alex Smith / Brendan Kehoe
USENET readers can currently receive CuD as alt.society.cu-digest.

The application and affidavit for the search warrant for Steve Jackson

Games (Case #A-90-54m), dated February 28, 1990, and signed by U.S. Magistrate Stephen H. Capelle in Austin Texas and Special Agent Timothy M. Foley of the U.S. Secret Service, has been released. The application alleges violations of Title 18 USC Sections 2314 and 1030 and was issued in the U.S. District Court (Western District of Texas).

We have retyped it, and there may be some typographical errors, but we have done our best to recreate it as is.

There are several features about the affidavit. First, the bulk of it is repititious and simply establishes the credentials of the investigators, summarizes basic terms, and provides general background that seems inconsequential in linking the persons to be searched to any substantive criminal activity. It should also be remembered that the "$79,449.00" document in question was shown to contain nothing of substance that is not available to the general public for under $14. Further, to our knowledge, there is no evidence, contrary to suggestions, that E911 software was obtained.

Most troublesome is the interpretation given to attached logs from The Phoenix Project that creates a conspiratorial scenario from a few ambiguous messages. While imaginative use of narrative is admirable in fiction, its use as a weapon of power is dangerous. At root, Steve Jackson Games was raided because an employee ran a BBS that made available, as did perhaps thousands of others BBSs nationwide, Phrack. The employee was also accused of being part of a "fraud scheme" because he had the temerity to explain what a Kermit protocol is in a two line message.

Perhaps Agent Foley is competent, but in reviewing this warrant questions arise regarding the raid on SJG that should not go unanswered.

++++++++++++++++++++++++++++

ATTACHMENT A

2700 "A" Metcalfe Road is located in the city of Austin, State of Texas, County of Travis. Said address is a two-story square building measuring approximately 50 feet on a side located on the south side of Metcalfe Street.

The bottom story is multi-colored brick face and the upper story is white wood frame construction.

A balcony surrounds the upper story. The address "2700A" is on two sides in white letters, and the numbers are approximately ten inches high. An outside wooden stairway connects the floors on the south side of the building. The driveway is of gravel. A large all-metal warehouse-type building is immediately behind the

address.

(End Attachment A)

++++++++++++++++

ATTACHMENT B

Computer hardware (including, but not limited to, central processing unit(s), monitors, memory devices, modem(s), programming equipment, communication equipment, disks, and prints) [sic] and computer software (including but not limited to, memory disks, floppy disks, storage media) and written material and documents relating to the use of the computer system (including networking access files), documentation relating to the attacking of computers and advertising the results of computer attacks (including telephone numbers and licensing documentation relative to the computer programs and equipment at the business known as Steve Jackson Games which constitute evidence, instrumentalities and fruits of federal crimes, including interstate transportation of stolen property (18 USC 2314) and interstate transportation of computer access information (18 USC 1030 (a)(6)). This warrant is for the seizure of the above described computer and computer data and for the authorization to read information stored and contained on the above described computer and computer data.

(End Attachment B)

++++++++++++++++++++++++

State of Texas)
) ss
County of Travis)

AFFIDAVIT

1. I, Timothy Foley, am a Special Agent of the United States Secret Service and have been so employed for the past two years. I am presently assigned to the United States Secret Service in Chicago. Prior to that I was employed as an attorney practicing in the City of Chicago and admitted to practice in the State of Illinois. I am submitting this affidavit in support of the search warrants for the premises known as: (a) the residence of Loyd Dean Blankenship, 1517G Summerstone, Austin, Texas; (b) the employment location of Blankenship, the business known as Steve Jackson Games, 2700-A Metcalfe Road, Austin Texas; and (c) the residence of Chris Goggans, 3524 Graystone #192, Austin, Texas.

SOURCES OF INFORMATION

2. This affidavit is based on my investigation and information provided to me by Special Agent Barbara Golden of the Computer Fraud Section of the United States Secret Service in Chicago and by other agents of the United States Secret Service.

3. I have also received technical information and investigative assistance from the experts in the fields of telecommunications, computer technology, software development and computer security technology, including:

a. Reed Newlin, a Security Officer of Southwestern Bell, who has numerous years of experience in operations,

maintenance and administration of telecommunications systems as an employee of the Southwestern Bell Telephone Company.

b. Henry M. Kluepfel, who has been employed by the Bell System or its divested companies for the last twenty-four years. Mr. Kluepfel is presently employed by Bell Communications Research, (Bellcore) as a district manager responsible for coordinating security technology and consultation at Bellcore in support of its owners, the seven regional telephone companies, including Bell South Telephone Company and Southwestern Bell Telephone Company. Mr. Kluepfel has participated in the execution of numerous Federal and State search warrants relative to telecommunications and computer fraud investigations. In addition, Mr. Kluepfel has testified on at least twelve occasions as an expert witness in telecommunications and computer-fraud related crimes.

c. David S. Bauer, who has been employed by Bell Communications Research (Bellcore) since April 1987. Mr. Bauer is a member of the technical staff responsible for research and development in computer security technology and for consultation in support of its owners, the seven regional telephone companies, including Bell South. Mr. Bauer is an expert in software development, communications operating systems, telephone and related security technologies. Mr. Bauer has conducted the review and analysis of approximately eleven computer hacking investigations for Bellcore. He has over nine years professional experience in the computer related field.

Violations Involved

4. 18 USC 2314 provides federal criminal sanctions against individuals who knowingly and intentionally transport stolen property or property obtained by fraud, valued at $5,000 or more

ininterstate commerce. My investigation has revealed that on or about February 24, 1989, Craig Neidorf transported a stolen or fraudulently obtained computerized text file worth approximately $79,000.000 from Columbia, Missouri, through Lockport, Illinois to Austin, Texas to Loyd Blankenship and Chris Goggans.

5. 18 USC 1030 (a)(6) and (b) provide federal criminal sanctions against individuals who knowingly and with intent to defraud traffic or attempt to traffic, in interstate commerce, in passwords or similar information through which a computer may be accessed without authorization. My investigation has revealed that on or about January 30, 1990, Loyd Blankenship and Chris Goggans attempted to traffic in illegally obtained encrypted passwords received from other computer hackers. My investigation has further revealed that, through the use of sophisticated decryption equipment and software, they planned to decrypt the encrypted passwords provided by the hackers. They then planned to provide the original hackers with the decrypted passwords which they in turn could use to illegally access previously guarded computers.

DEFINITIONS

6. COMPUTER HACKERS/INTRUDERS - Computer hackers or intruders are individuals involved with the unauthorized access of computer systems by various means. The assumed names used by the

hackers when contacting each other are referred to as "hacker handles."

7. BULLETIN BOARD SYSTEM (BBS) - A bulletin board system (also referred to as a "Bulletin board" or "BBS") is an electronic bulletin board accessible by computer. Users of a bulletin board may leave messages, data, and software readable by others with access to the bulletin board. Bulletin board readers may copy, or "download," onto their own machines material that appears on a bulletin board. Bulletin boards typically are created and maintained by "systems operators" or "system administrators". Hackers frequently use bulletin boards to exchange information and data relating to the unauthorized use of computers.

8. E911 - E911 means the enhanced 911 telephone service in universal use for handling emergency calls (police, fire, ambulance, etc.) in municipalities. Dialing 911 provides the public with direct access to a municipality's Public Safety Answering Point (PSAP). Logistically, E911 runs on the public telephone network with regular telephone calls into the telephone company switch. However, incoming 911 calls are given priority over all other calls. Then the 911 call travels on specially dedicated telephone lines from the telephone company's switch to

the fire, police and emergency reaction departments in the city closest to the location of the caller. It is essential for the emergency unit to know the location of the caller, so one of the most important parts of the system is the Automatic Location Identifier (ALI), which automatically locates where the

telephone call originates, and the Automataic Number Identification (ANI), which holds the telephone number of the calling party even if the caller hangs up. The E911 system of Bell South is described in the text of a computerized file program and is highly proprietary and closely held by its owner, Bell South. The file describes the computerized control, operation and maintenance of the E911 system.

9. ELECTRONIC MAIL - Electronic mail, also known as e-mail, is a common form of communication between individuals on the same or on separate computer systems. Persons who may send or receive electronic mail are identified by an electronic mail address, similar to a postal address. Although a person may have more than one electronic mail address, each mail address identifies a person uniquely.

10. LEGION OF DOOM - At all times relevant herein, the Legion of Doom, (LOD), was a closely knit group of computer hackers involved in:

a. Disrupting telecommunications by entering telephone switches and changing the routing on the circuits of the computers.

b. Stealing propriety (sic) computer source code and information from individuals that owned the code and information

c. Stealing credit information on individuals from credit bureau computers.

d. Fraudulently obtaining money and property from companies by altering the computerized information used by the companies.

e. Disseminating information with respect to their methods of attacking computers to other computer hackers in an effort to avoid the focus of law enforcement agencies and telecommunication security experts.

11. PASSWORD ENCRYPTION - A password is a security device that controls access to a computer, (log on privileges) or to special portions of a computer's memory. Encryption further limits access to a computer by converting the ordinary language and/or numerical passwords used on a computer into cipher or code. Decryption is the procedure used to transform coded text into the original ordinary language and/or numerical format.

12. TRANSFER PROTOCOL - transfer protocol is a method of transferring large files of information from one computer to another over telephone lines. Using a transfer protocol a file is uploaded (sent) and downloaded (received). This transfer procedure breaks blocks of data into smaller packages for transmission and insures that each block of data is an error free copy of the original data. Transfer protocols may also encode and decode transmissions to insure the privacy of the transferred information.

INVESTIGATION OVERVIEW

13. My investigation to date has disclosed that computer hacker Robert Riggs of the Legion of Doom, (LOD), stole the highly proprietary and sensitive Bell South E911 Practice text file from Bell South in Atlanta, Georgia in about December, 1988 and that

this stolen document was distributed in "hacker" newsletters through the use of e-mail. These newsletters included the "Phrack" newsletter issue #24 distributed in February, 1989 by Crig Neidorf to LOD members, including Loyd Blankenship and Chris Goggans of Austin, Texas. The E911 Practice was posted on the "Phoenix Project" BBS, in January, 1990, so that anyone with access to the BBS could download a copy of the E911 Practice onto any other computer. The "Phoenix Project" BBS is run jointly by co-systems operators Loyd Blankenship, (hacker handle, The Mentor), and Chris Goggans, (hacker handle, Eric [sic] Bloodaxe), who both have sent e-mail communications identifying themselves as members of LOD. My investigation has also disclosed that Loyd Blankenship and Chris Goggans, through their hacker BBS "Phoenix Project," have established a password decryption service for hackers who had obtained encrypted passwords from computers they had been attacking.

THEFT OF E911 TEXT FILE

14. In March, 1988, Bell South developed a sophisticated new program which describes in great detail the operation of the E911 system and the 911 support computer in Sunrise, Florida that controls ALI and ANI information. This program, which was enginered at a cost of $79,449.00, was locked in a secure computer (AIMSX) in Bell South's corporate headquarters in Atlanta, Georgia. The document was and is highly proprietary and contained the following warning:

NOTICE: NOT FOR USE OR DISCLOSURE OUTSIDE
BELL SOUTH OR ANY OF ITS SUBSIDIARIES EXCEPT
UNDER WRITTEN AGREEMENT.

15. In July, 1989, Robert Riggs apartment in Decatur, Georgia was searched by United States Secret Service agents from Atlanta pursuant to a federal search warrant.

16. At the time of the search, Riggs, (hacker handle, The Prophet), was interviewed by Special Agent James Cool of the USSS-Atlanta and representatives of Bell South from Atlanta. During this extensive interview, Riggs admitted that he illegally gained remote access into Bell South's AIMSX computer through an account to which access was not secured by a password, and that once on the machine he executed a program designed to search for passwords and to obtain other account names on the computer. He stated that once he was on the computer, he found the E911 protocol document and downloaded it from the Bell South computer to his home computer. He subsequently uploaded the E911 file from his home computer to a computer bulletin board. (He did not give the agents the name of the bulletin board).

17. Riggs' admissions were corroborated by interviews with Rich Andrews, the operator of the computer bulletin board known as JOLNET BBS in Lockport, Illinois. Andrews disclosed that in about January, 1989, a hacker known to him by the handle PROPHET uploaded an E911 program with bell South proprietary markings onto his BBS. This program was then downloaded from the BBS to another hacker known to him by the handle Knight Lightning (Craig Neidorf).

PHRACK PUBLICATION

18. On January 18, 1990, pursuant to a federal grand jury subpoena, I received documents from the administration of the University of Missouri regarding computer publications of Craig Neidorf, a student at University of Missouri and Randly Tishler, a former student at University of Missouri, (hacker handle, Taran King), which showed that Neidorf and Tishler were publishing the computer hacker newsletter entitled "Phrack" which they were distributing to computer hackers around the United States through the use of the University of Missouri account on a telecommunication network called Bitnet.

19. On January 18, 1990, Security Officer Reed Newlin of Southwestern Bell Telephone and I interviewed Craig Neidorf at the Zeta Beta Tau Fraternity House at Columbia, Missouri. During the course of the interview, Neidorf admitted to me and Security Officer Newlin that he used the hacker handle Knight Lightning; that he and Randy Tishler were the publishsers of two hacker newsletters entitled "Phrack" and "Pirate."

20. Also during the course of this interview, Neidorf

admitted that he had a copy of a hacker tutorial regarding the operation of the E911 system in his room. He admited that he had edited the E911 Practice into a hacker tutorial. He also admitted that he knew that the E911 Practice had been stolen from a telecommunications company by Robert J. Riggs and that the tutorial, (the edited E911 Practice File), had been published in the Phrack newsletter issue 24. At this point of the interview,

Neidorf excused himself, saying he was going to his room, and he returned moments later with a floppy disk containing the copy of the E911 document published in Phrack magazine.

21. In addition to Neidorf's admission that he knew the E911 tutorial had been stolen, my investigation has revealed other facts reflecting that Neidorf was aware that the E911 data received from Riggs in Atlanta was stolen. In July, 1989, I reviewed documentation received from Rich Andrews, the system administrator of the JOLNET BBS. Included in the documentation was an edited version of the E911, the document received from Neidorf, dated January 23, 1989, which included the following notation on his version:

> NOTICE: NOT FOR USE OR DISCLOSURE OUTSIDE
> BELLSOUTH OR ANY OF ITS SUBSIDIARIES EXCEPT
> UNDER WRITTEN AGREEMENT. (WHOOPS)

22. Distribution records of Phrack 24 recovered from Richard Andrews in Lockport in July 1989 reflect that copies of this newsletter containing the proprietary E911 information and the proprietary markings from Bell South were forwarded from Neidorf's computer in Colombia [sic], Missouri to Loyd Blankenship's computer in Austin, Texas on or about February 24, 1989.

23. I have personally examined the Phrack newsletter number 24 and observed that the newsletter does in fact contain a slightly edited copy of the stolen Bell South E911 Practice text file with the warning:

> NOTICE: NOT FOR USE OR DISCLOSURE OUTSIDE

> BELLSOUTH OR ANY OF ITS SUBSIDIARIES EXCEPT
> UNDER WRITTEN AGREEMENT. (WHOOPS)

REPUBLICATION OF E911 BY PHOENIX PROJECT

24. On February 26, 1990, Hank Kluepfel of Bellcore advised me that the Phoenix Project BBS run by Loyd Blankenship and Chris Goggans was in operation on January 15, 1990. Mr. Kluepfel advised that he had made this determination by successfully logging on to Phoenix Project at telephone number 512-441-0229 on about January

30, 1990 and observing messages dated from January 15, 1990 to January 30, 1990, on the BBS. Mr. Kluepfel also advised me that the BBS system information identified the Mentor and Erik Bloodaxe as the system administrators on the BBS.

25. On February 14, 1990, Mr. Kluepfel advised me that after accessing the Phoenix Project BBS, he had gone to the Phrack sub-menu of the BBS and observed Phrack 24 on the menu. Mr. Kluepfel further advised me that upon review of Phrack 24, he observed that the Bell South E911 Practice text file was still in the edition carried by the Phoenix Project BBS.

26. On February 14, 1990, Mr. Kluepfel advised me that he had downloaded a copy of Phoenix Project's user list (its electronic mailing list) and that it reflected that seeral of the hackers on the list of users were located in the Northern District of Illinois.

PHOENIX PROJECT DECRYPTION SERVICE

27. On February 14, 1990, Mr. Kluepfel advised me that on January 23, 1990, the co-systems administrator on the Phoenix Project BBS, Erik Bloodaxe, had published a notice that the BBS was beginning a new decryption service. Bloodaxe invited the readers of the newsletter to send the BBS encrypted passwords for any UNIX or Prime computer system, and the system administrators would decrypt the passwords and return them. Bloodaxe also indicated that the systemes administrators would probably access the computer using the password as well. In a later message on January 26, 1990, The Mentor responded to a question about a transfer protocol that had been set out, but not explained in Bloodaxe's notice, indicating his involvement in the decryption scheme.

28. On February 14, 1990, Mr. Kluepfel advised me that the password file decryption service offered by the Phoenix Project provided computer hackers with information through which a computer could be acessed without authorization under the meaning of 18 USC 1030 (a)(6) and (b) and constituted a threat to Bellcore's client companies including Bell South.

IDENTIFICATION OF BLANKENSHIP AND GOGGANS

29. Among the documents that had been printed out from the University of Missouri computers, which I received from the University of Missouri computers, which I received from the administration of the University of Missouri, were lists of hackers and their corresponding real names. On that list were the names of Loyd Blankenship and Chris Goggans and their respective hacker handles of The Mentor and Erik Bloodaxe.

30. Among the documents seized in the search of Neidorf's

house were phone lists which included the full names of Loyd Blankenship and Chris Goggans and identified them as The Mentor and Erik Bloodaxe, respectively.

31. On February 6, 1990, Mr. Kluepfel provided me with copies of a Phrack newsletter which contained a September 23, 1989, profile of computer hacker Erik Bloodaxe. The profile indicated that the Erik Bloodaxe's real name was Chris, that he was 20 years old, 5'10", 130 pounds, that he had blue eyes, brown hair and that he used various computers including an Atari 400, various computer terminals with limited computing capability that are or can be linked to a central computer, and a CompuAid Turbo T. The profile reflects that Erik Bloodaxe was a student in computer science at the University of Texas in Austin.

32. On February 6, 1990, Mr. Kluepfel provided me with a copy of Phrack containing a January 18, 1989 profile of the computer hacker known as The Mentor. The profile indicated that the Mentor's real name was Loyd, that he was 23 years old, 120 pounds, 5'10", that he had brown hair, brown eyes and that he had owned a TRS-80, an Apple IIe, an Amiga 1000, and a PC/AT.

33. The identification of Loyd Blankenship as The Mentor in the Phrack profile was corroborated on February 22, 1990, by information provided by Larry Coutorie an inspector with campus security at the University in Austin, Texas who advised me that his review of locator information at the University of Texas in Austin disclosed current drivers license information on

Loyd Dean Blankenship reflecting that Blankenship resides at 1517G Summerstone, in Austin, Texas, telephone number 512-441-2916 and is described as a white, male, 5'10", with brown hair and brown eyes. He further advised that Blankenship is employed at Steve Jackson Games, 2700-A Metcalfe Road, Austin, Texas where he is a computer programmer and where he uses a bulletin board service connected to telephone number 512-447-4449.

34. According to telephone company records the telephone number 512-441-0229, the number for the Phoenix Project BBS, is assigned to the address 1517 G Summerstone, Austin, Texas, which is the residence of Loyd Blankenship.

35. Hank Kluepfel has advised me that he has loged on to the BBS at 512-447-4449 and that The Mentor is listed as the systems operator of the BBS. Mr. Kluepfel further advised me that the user list of that BBS contains the name of Loyd Blankenship and others known to Mr. Kluepfel has hackers. Also, Mr. Kluepfel observed that Loyd Blankenship is a frequent user of the BBS.

36. Similarly, the identification of Chris Goggans as the Erik Bloodaxe described in the Phrack profile was corroborated on February 22, 1990, by Larry Coutorie who advised me that his

review of locator information at the University of Texas with respect to Chris Goggans disclosed that Goggans resides at 3524 Graystone #192, in AUstin, Texas and that his full name is Erik Christian Goggans. Goggans, who goes by the name Chris, is a white, male, with blond hair and blue eyes date of birth 5/5/69, 5'9", 120 pounds.

37. On February 19, 1990, I was advised by Margaret Knox, Assistant Director of the Computation Center, University of Texas, Austin, Texas, that a young man presented himself to her as Chris Goggans in response to the University sending a notification of the Grand Jury subpoena for University records pertaining to Chris Goggans to Chris Goggans at 3524 Graystone #192, Austin, Texas. The young man also told her that he was Erik Bloodaxe of the Legion of Doom.

Locations to be Searched

38. Based on the above information and my own observations, I believe that the E911 source code and text file and the decryption software program are to be found in the computers located at 1517G Summerstone, Austin, Texas, or at 2700-A Metcalfe Road, Austin, Texas, or at 3524 Graystone #192, Austin, Texas, or in the computers at each of those locations.

39. The locations to be searched are described as: the premises known as the residence of Loyd Dean Blankenship, 1517G Summerstone, Austin, Texas; the employment location of Blankenship, the business known as Steve Jackson Games, 2700-A Metcalfe Road, AUstin, Texas; and the residence of Chris Goggans, 3524 Graystone #192, Austin, Texas. Those locations are further described in Attachment A to this Affidavit for Search Warrant.

Evidence To Be Found

40. On February 2, 1990, Jerry Dalton of AT&T advised me that based upon his background, experience and investigation in this

case and investigating approximately 50 other incidents this year involving the unauthorized use of other computer systems, including individuals that run computer bulletin boards, these individuals typically keep and use the following types of hardware, software and documents to execute their fraud schemes and operate their computers and computer bulletin boards:

a. Hardware - a central processing unit, a monitor, a modem, a key board, a printer, and storage devices (either cartridge tapes, 9-track magnetic tapes, floppy disks or axillary [sic] disk units), telephone equipment (including) automatic dialing equipment, cables and connectors), tape

drives and recording equipment.

b. Software - hard disks and floppy disks containing computer programs, including, but not limited to software data files, electronic mail files, UNIX software and other AT&T proprietary software.

c. Documents - computer related manuals, computer related textbooks, looseleaf binders, telephone books, computer printout, cassette tapes, videotapes and other documents used to access computers and record information taken from the computers during the above referred breakins. Financial and licensing information with respect to the computer hardware and software.

41. Based on the above information and my own observation, I believe that at the premises known as the residence of Loyd Dean Blankenship, 1571G Summerstone, Austin, Texas; the employment location of Blankenship, the business known as Steve Jackson Games, 2700-A Metcalfe Road, Austin, Texas; and the residence of Chris Goggans, 3524 Graystone, #192, Austin Texas there is computer hardware (including central processing unit(s), monitors, memory devices, (modem(s), programming equipment, communication equipment, disks, prints and computer software (including but not limited to memory disks, floppy disks, storage media) and written material and

documents relating to the use of the computer system (including networking access files, documentation relating to the attacking of computer and advertising the results of the computer attack (including telephone numbers and location information). This affidavit is for the seizure of the above described computer and computer data and for the authorization to read information stored and contained on the above described computer and computer data which are evidence of violations of 18 USC 2314 and 1030, as well as evidence, instrumentalities or fruits of the fraud scheme being conducted by the operator of the computer at that location.

42. Request is made herein to search and seize the above described computer and computer data and to read the information contained in and on the computer and computer data.

(signature of) Timothy M. Foley
Special Agent Timothy Foley
United States Secret Service

Sworn and Subscribed to before
me this 28th day of February, 1990

(signature of) Stephen H. Capelle
UNITED STATES MAGISTRATE

(END OF SEARCH AFFIDAVIT)

++
++

A document attached to the search affidavit reproduced 17 messages from The Phoenix Project written from Jan. 23 - Jan. 29, 1990. We have retyped messages 13/17, but substituted the original posts (18/29) from TPP logs we have obtained. The differences in message numbers (eg 13/58 from Henry Kluepfel's logs, or our source's logs, eg, 22/47) reflect that the notes were captured on different days. We have compared the logs from both our source and the document, and they are identical. Hence, the difference in capturing dates is of no consequence.

There are several points that should be considered in reading the logs:

1. The affidavit claims that the logs substantiate the claim that an encryption service existed. In fact, they do no such thing. The claim is based primarily on message 13 (Jan 23), which includes the comment "What do you people think? Bad idea? Good idea? Hell...It is just another attempt by me to piss everyone off."

2. The bulk of these messages are inconsequential general discussions, and include brief discussion of transfer protocols.

3. Timothy Foley's "evidence" that The Mentor is involved in the situation is message 23, in which The Mentor is "guilty" of saying that Kermit is a 7-bit transfer protocol, is found on mainframes, and works through outdials. From this, Foley says:

> In a later message on January 26, 1990, the Mentor responded to a question about a transfer protocol that been set out, but not explained in Bloodaxe's notice, indicating his involvement in the decryption scheme (#27, p. 12).

4. The messages before and after these dates are general, and there is little substantive discussion of the "decryption service."

It appears that Loyd Blankenship is "guilty" of posting phracks on The Phoenix Project, as are perhaps thousands of other sysops across the country, and of the "criminal act" of summarizing Kermit.

We will leave it to others to judge and comment upon the logic and quality of the document(s).

++
(The following is the first page of a 3 page document attached to the affidavit. It has been retyped from the original).
++

New user pw= GUNSHIP

13/58: things...
Name: Erik Bloodaxe #2
Date: Tue Jan 23 22:57:29 1990
I think it's time for your friend at The Legion of Doom to start a new service...(with great help from friends)
Decryption service! On any unix or Prime, send the etc/passwd file, or the UAF file to the sysop directory, and you will be mailed back the encrypted UAF file to the sysop directory, and you will be mailed back the encrypted passwords...(on UNIX any pw that the deszip could bust)
The Prime UAF must be in binary, so kermit it from the site, and xmodem it here.
In return, we will not distribute any information gained from your site, but we will probably look around it anyway...but it will remain between you and us.
What do you people think? Bad idea? Good idea? Hell...It is just another attempt by me to piss everyone off.
->ME

14/58: aha..!
Name: Phoenix #17
Date: Wed Jan 24 01:30:35 1990
ummm...hmmm
(doesn't know what to say..)

15/58: Heck
Name: The Parmaster #21
Date: Wed Jan 24 07:48:01 1990
    Personally i like it :-)
Jason.

16/58: Decryption
Name: Grey Owl #10
Date: Wed Jan 24 19:10:52 1990

I think it's a great idea. I get a whole shitload of passwd files and some UAF files too. |||_____got!
grey owl

17/58: Just a couple of questions...
Name: Konica #47
Date: Wed Jan 24 23:41:13 1990
Well since the feds know this is a hacker board whats stopping them from tracing every incoming call to Pheonix Project and getting all the #'s, then monitoring then for illegal activity?

And just say I was calling through my personal calling card....What would they get as the incomming #?
If I had a DNR on my line is there any way I could find out?
Sorry about this but I am not as good as most of you (except for the guy that keeps posting codes) and the only way I am going to learn is by trying shit out and asking questions...
Hope this is the right sub for these questions....

+++++++++++++++
(The following are the actual logs; Typos were not removed)
+++++++++++++++

18/47: vv
Name: Dtmf #27
Date: Thu Jan 25 03:22:29 1990

RE: Just a couple of questions...

To check the DNR the best bet woud be to call bell security, or the SCC

19/47: well..
Name: Phoenix #17
Date: Thu Jan 25 07:27:43 1990

nothing stops them from tracing..
I dont know how it works there.. but down here all traces are illegal unless they are for drug/murder reasons.. (well not traces, but taps are..)

20/47: Feds...
Name: Erik Bloodaxe #2
Date: Thu Jan 25 17:05:35 1990

Absolutely nothing would stop them from collecting all local calls, and/or any longdistance company records of calls coming into this number...in fact, I

kind of expect them to at least get all local calls here...hell Austin is all ess...most of them 5's...(I think...maybe 1's)

However, I doubt that tapping the data line is worth their while...especially when they can just log on and read everything anyway. And the mail just isn't that spectacular...

In any case, all calls here made by legal means are legaal, so don't worry about it. Just because tee nature of this bbs isn't that of your average mainstream bbs, doesn't negate its legality. Information posted here is kept legal.

If you are truly worried about it, don't call, and sit home being paranoid.

Hell, I'm local...I call direct...and now I do it at 300 baud. Hell, I can almost tell what's being typed at 300 baud while listening to it...forget the data tap! Hehe, although a 300 baud data tap is SO simple to playback completely error free...at 1200 or 2400 you kind of have to get the recording levels just right...but 300 gives you plenty of room for error...

21/47: ess 1,5
Name: Dark Sun #11
Date: Thu Jan 25 20:14:00 1990

hey, whats the diff??? :-)
DS

22/47: decryption
Name: Silencer #31
Date: Thu Jan 25 23:35:01 1990

hmmm....like...you mean once you have an account...read the user file and then you will deencrypt all the passcodez...sounds good....but what the fuck is kermit...
- Silencer

23/47: kermit
Name: The Mentor #1
Date: Fri Jan 26 10:11:23 1990

Kermit is a 7-bit transfer protocol that is used to transfer files to/from machines. It is mostly found on mainframes (it's a standard command on VAX,

for instance). Kermit has the added advantage of being able to work through an outdial (because it is 7-bit).

Mentor

24/47: Kermit
Name: Sicilumm Thorne #28
Date: Fri Jan 26 11:20:10 1990

Kermit is merely another transfer protocol like Sealink, Xmodem, Modem7, Zmodem, et cetera.

Its relatively slow, but was thought to be better than Xmodem, due to its capabilties. (Don't remember what they are, I use Zmodem).

Sic.

25/47: my kermit
Name: Ravage #19
Date: Fri Jan 26 12:24:21 1990

lets me set it at 8 bits also. just another trivial note.

26/47: from what I know...
Name: Dark Sun #11
Date: Fri Jan 26 16:26:55 1990

kermit was originally designed to allow transmission of data across 2 computers running with different parity settings.
DS

27/47: and..
Name: Phoenix #17
Date: Sat Jan 27 07:28:45 1990

as a major disadvantage.. it is damn slow!

Phoenix

28/47: Well....
Name: Johnny Hicap #45
Date: Sat Jan 27 21:28:18 1990

No one answered that question (forget who posted it) that if he was calling through a calling card is it possible to get the number of the person who called even he was calling through hs calling card? What would they get as the number comming in? Would they get the card? Of course then they would just see who owns it.

JH!

29/47: more Kermit BS
Name: Grey Owl #10
Date: Sat Jan 27 23:53:57 1990

Kermit is slower than Xmodem, BTW. The packets are smaller (usually 64 bytes) and the error-checking is shot to hell with any line noise. It's better than ASCII though!

grey owl

****
** END OF CuD #2.11 **
****

Formation documents and mission statement for the EFF

ELECTRONIC FRONTIER FOUNDATION INTRODUCED IN WASHINGTON 7-10-90

10 July 90 --- Mitch Kapor, the founder of Lotus Development Corp., announced at a news conference this morning that his newly formed Electronic Frontier Foundation is giving $275,000 to Computer Profes-sionals for Social Responsibility to expand their program on computers and civil liberties.

CPSR will host a series of policy round-tables in Washington during the next two years, to bring together lawmakers, computer users, industry representatives, and law enforcement officials "to ensure that our civil liberties protections are not lost amidst policy confusion about the use of new computer technologies," according to a press release.

"CPSR also plans to develop policy papers on computer and civil liberties, to oversee the Government's handling of computer crime investigations, and to act as an information resource for organizations and individuals interested in civil liberties issues."

In addition, Kapor said EFF will foot the legal costs to recover a computer bulletin-board system seized about 4 months ago from Steve Jackson Games of Austin, Texas. Reasons for the seizure are still unclear, since no charges have yet been filed, and the warrant for the seizure was sealed by the court.

During the raid the Secret Service also confiscated drafts of a role-playing game that SJG was about to release, believing it to be a training manual for computer crime. The game - GURPS Cyberpunk - has since been published (with modifications), but this morning Jackson asserted that the delay and the work needed to reconstruct the game cost his company some $125,000.

"I am a horror story," he began. Picking up on metaphors used by John Perry Barlow, who preceded him to the microphone, Jackson called himself "one of the homesteaders on the electronic frontier... One day I came home to find the barn burned down, the horses set loose...and the culprits who did it weren't desperados. They were the cavalry!"

Jackson's lawyer, Harvey Silverglate, added that taking the BBS that SJG

used for customer support was analogous to seizing presses from the New York Times. Terry Gross, a lawyer for Craig Neidorf, pressed the point further as he told of his client's problems. Neidorf, a college student who edits an electronic newsletter called "Phrack," has been charged with perpetrating a "wire fraud scheme" by electronically receiving "stolen goods" (a BellSouth internal memo describing 911 system features) and transmitting a digest of the memo as an article in Phrack.

"This is like prosecuting the New York Times or the Washington Post for wire fraud for publishing the Pentagon Papers," Gross argued. These charges wouldn't have been brought if Phrack were published on paper, he added. Some of the charges against Neidorf are specific to electronic transmission.

In thanking EFF for the grant, Marc Rotenberg, CPSR's spokesman in Washington, said the Jackson and Neidorf cases epitomize the tough moral and legal issues we'll be grappling with for years to come. Gross, Silverglate and Rotenberg agreed that these early cases are especially important because they may set precedents.

Kapor repeatedly emphasized that the Electronic Freedom Foundation isn't a "hackers defense fund." "Unauthorized intrusion into computer systems is improper behavior and should be illegal," he declared. EFF's purpose is to see that First Amendment rights aren't trampled in overreaction to real or imaginary threats posed by computer crackers.

A basic feature of today's "information society" is anxiety about our dependence on electronic media whose workings we don't understand, Kapor explained. Barlow added that we're on "the learning curve of Sisyphus": technology is evolving faster than we can understand, and it always will be.

Kapor suggested that hackers are increasingly portrayed as threatening sorcerers mainly because they don't share most people's anxiety and ignorance about computer technology. He described the current anti-hacker hysteria in terms of the sci-fi movie classic, "The Forbidden Planet": the monsters, it turns out in the end, were all Dr. Morbius' projections.

"Hacker" used to be a term of high praise, Kapor pointed out. Hackers also created the multi-billion dollar personal computer industry, so it is appropriate that EFF is funded by Kapor, Apple co-founder Steve Wozniak, and a "Silicon Valley pioneer" who wishes to remain unnamed.

Kapor warned that "polarization and misunderstanding" of hackers could slow public acceptance of computer networks as a valuable tool in everyday life. If we want useful nets for everyone, he said, we must make them both open AND secure - a programming feat that calls for hacker-type ingenuity.

To improve public understanding of electronic networks and the resources they provide, Kapor announced that EFF will sponsor the development of "intelligent front-ends" for UNIX e-mail, to be used on Apple/Mac and DOS machines. This software would be available at little or no cost, and so easy to use that even a "hacker's mother" won't find it intimidating. Making networks more accessible will greatly expand the market for hardware and software, he concluded.

The Electronic Frontier Foundation can be contacted at One Cambridge Center, Suite 300, Cambridge, MA 02142 (617-577-1385; fax 617-225-2347; Internet eff@well.sf.ca.us.

FOR IMMEDIATE RELEASE July 10, 1990

CPSR TO UNDERTAKE EXPANDED CIVIL LIBERTIES PROGRAM

Contact: Marc Rotenberg (202) 775-1588

Washington, D.C., July 10, 1990 -- Computer Professionals for Social Responsibility (CPSR), a national computing organization, announced today that it would receive a two-year grant in the amount of $275,000 for its Computing and Civil Liberties Project. The Electronic Frontier Foundation (EFF),founded by Mitchell Kapor, made the grant to expand ongoing CPSR work on civil liberties protections for computer users.

At a press conference in Washington today, Mr. Kapor praised CPSR's work, "CPSR plays an important role in the computer community. For the last several years, it has sought to extend civil liberties protections to new information technologies. Now we want to help CPSR expand that work."

Marc Rotenberg, director of the CPSR Washington Office said, "We are obviously very happy about the grant from the EFF. There is a lot of work that needs to be done to ensure that our civil liberties protections are not lost amidst policy confusion about the use of new computer technologies."

CPSR said that it will host a series of policy round tables in Washington, DC, during the next two years with lawmakers, computer users, including (hackers), the FBI, industry representatives, and members of the computer security community. Mr. Rotenberg said that the purpose of the meetings will be to "begin a dialogue about the new uses of electronic media and the protection of the public interest."

CPSR also plans to develop policy papers on computers and civil

liberties, to oversee the Government's handling of computer crime investigations, and to act as an information resource for organizations and individuals interested in civil liberties issues.

The CPSR Computing and Civil Liberties project began in 1985 after President Reagan attempted to restrict access to government computer systems through the creation of new classification authority. In 1988, CPSR prepared a report on the proposed expansion of the FBI's computer system, the National Crime Information Center. The report found serious threats to privacy and civil liberties. Shortly after the report was issued, the FBI announced that it would drop a proposed computer feature to track the movements of people across the country who had not been charged with any crime.

"We need to build bridges between the technical community and the policy community," said Dr. Eric Roberts, CPSR president and a research scientist at Digital Equipment Corporation in Palo Alto, California. "There is simply too much misinformation about how computer networks operate. This could produce terribly misguided public policy."

CPSR representatives have testified several times before Congressional committees on matters involving civil liberties and computer policy. Last year CPSR urged a House Committee to avoid poorly conceived computer activity. "In the rush to criminalize the malicious acts of the few we may discourage the beneficial acts of the many," warned CPSR. A House subcommittee recently followed CPSR's recommendations on computer crime amendments.

Dr. Ronni Rosenberg, an expert on the role of computer scientists and public policy, praised the new initiative. She said, "It's clear that there is an information gap that needs to be filled. This is an important opportunity for computer scientists to help fill the gap."

CPSR is a national membership organization of computer professionals, based in Palo Alto, California. CPSR has over 20,000 members and 21 chapters across the country. In addition to the civil liberties project, CPSR conducts research, advises policy makers and educates the public about computers in the workplace, computer risk and reliability, and international security.

For more information contact:

Marc Rotenberg
CPSR Washington Office
1025 Connecticut Avenue, NW, Suite 1015
Washington, DC 20036 202/775-1588

Gary Chapman

CPSR National Office
P.O. Box 717
Palo Alto, CA 94302
415/322-3778

ELECTRONIC FRONTIER FOUNDATION - MISSION STATEMENT July 10, 1990

A new world is arising in the vast web of digital, electronic media which connect us. Computer-based communication media like electronic mail and computer conferencing are becoming the basis of new forms of community. These communities without a single, fixed geographical location comprise the first settlements on an electronic frontier.

While well-established legal principles and cultural norms give structure and coherence to uses of conventional media like newspapers, books, and telephones, the new digital media do not so easily fit into existing frameworks. Conflicts come about as the law struggles to define its application in a context where fundamental notions of speech, property, and place take profoundly new forms. People sense both the promise and the threat inherent in new computer and communications technologies, even as they struggle to master or simply cope with them in the workplace and the home.

The Electronic Frontier Foundation has been established to help civilize the electronic frontier; to make it truly useful and beneficial not just to a technical elite, but to everyone; and to do this in a way which is in keeping with our society's highest traditions of the free and open flow of information and communication.

To that end, the Electronic Frontier Foundation will:

1. Engage in and support educational activities which increase popular understanding of the opportunities and challenges posed by developments in computing and telecommunications.

2. Develop among policy-makers a better understanding of the issues underlying free and open telecommunications, and support the creation of legal and structural approaches which will ease the assimilation of these new technologies by society.

3. Raise public awareness about civil liberties issues arising from the rapid advancement in the area of new computer-based communications media. Support litigation in the public interest to preserve, protect, and extend First Amendment rights within the realm of computing and telecommunications technology.

4. Encourage and support the development of new tools which will

endow non-technical users with full and easy access to computer-based telecommunications.

The Electronic Frontier Foundation
One Cambridge Center, Cambridge, MA 02142
(617) 577-1385

eff@well.sf.ca.us

ACROSS THE ELECTRONIC FRONTIER

by: Mitchell Kapor and John Perry Barlow
Electronic Frontier Foundation
Washington, D.C.
July 10, 1990

Over the last 50 years, the people of the developed world have begun to cross into a landscape unlike any which humanity has experienced before. It is a region without physical shape or form. It exists, like a standing wave, in the vast web of our electronic communication systems. It consists of electron states, microwaves, magnetic fields, light pulses and thought itself.

It is familiar to most people as the "place" in which a long-distance telephone conversation takes place. But it is also the repository for all digital or electronically transferred information, and, as such, it is the venue for most of what is now commerce, industry, and broad-scale human interaction. William Gibson called this Platonic realm "Cyberspace," a name which has some currency among its present inhabitants.

Whatever it is eventually called, it is the homeland of the Information Age, the place where the future is destined to dwell.

In its present condition, Cyberspace is a frontier region, populated by the few hardy technologists who can tolerate the austerity of its savage computer interfaces, incompatible communications protocols, proprietary barricades, cultural and legal ambiguities, and general lack of useful maps or metaphors.

Certainly, the old concepts of property, expression, identity, movement, and context, based as they are on physical manifestation, do not apply succinctly in a world where there can be none.

Sovereignty over this new world is also not well defined. Large institutions already lay claim to large fiefdoms, but most of the actual

natives are solitary and independent, sometimes to the point of sociopathy. It is, therefore, a perfect breeding ground for both outlaws and vigilantes. Most of society has chosen to ignore the existence of this arising domain. Every day millions of people use ATM's and credit cards, place telephone calls, make travel reservations, and access information of limitless variety. . . all without any perception of the digital machinations behind these transactions.

Our financial, legal, and even physical lives are increasingly dependent on realities of which we have only dimmest awareness. We have entrusted the basic functions of modern existence to institutions we cannot name, using tools we've never heard of and could not operate if we had.

As communications and data technology continues to change and develop at a pace many times that of society, the inevitable conflicts have begun to occur on the border between Cyberspace and the physical world.

These are taking a wide variety of forms, including (but hardly limited to) the following:

I. Legal and Constitutional Questions

What is free speech and what is merely data? What is a free press without paper and ink? What is a "place" in a world without tangible dimensions? How does one protect property which has no physical form and can be infinitely and easily reproduced? Can the history of one's personal business affairs properly belong to someone else? Can anyone morally claim to own knowledge itself?

These are just a few of the questions for which neither law nor custom can provide concrete answers. In their absence, law enforcement agencies like the Secret Service and FBI, acting at the disposal of large information corporations, are seeking to create legal precedents which would radically limit Constitutional application to digital media.

The excesses of Operation Sun Devil are only the beginning of what threatens to become a long, difficult, and philosophically obscure struggle between institutional control and individual liberty.

II. Future Shock

Information workers, forced to keep pace with rapidly changing technology, are stuck on "the learning curve of Sisyphus." Increasingly, they find their hard-acquired skills to be obsolete even before they've been fully mastered. To a lesser extent, the same applies to ordinary citizens who correctly feel a lack of control over their own lives and identities.

One result of this is a neo-Luddite resentment of digital technology from which little good can come. Another is a decrease in worker productivity ironically coupled to tools designed to enhance it. Finally, there is a spreading sense of alienation, dislocation, and helplessness in the general presence of which no society can expect to remain healthy.

III. The "Knows" and the "Know-Nots"

Modern economies are increasingly divided between those who are comfortable and proficient with digital technology and those who neither understand nor trust it. In essence, this development disenfranchises the latter group, denying them any possibility of citizenship in Cyberspace and, thus, participation in the future.

Furthermore, as policy-makers and elected officials remain relatively ignorant of computers and their uses, they unknowingly abdicate most of their authority to corporate technocrats whose jobs do not include general social responsibility. Elected government is thus replaced by institutions with little real interest beyond their own quarterly profits.

We are founding the Electronic Frontier Foundation to deal with these and related challenges. While our agenda is ambitious to the point of audacity, we don't see much that these issues are being given the broad social attention they deserve. We were forced to ask, "If not us, then who?"

In fact, our original objectives were more modest. When we first heard about Operation Sun Devil and other official adventures into the digital realm, we thought that remedy could be derived by simply unleashing a few highly competent Constitutional lawyers upon the Government. In essence, we were prepared to fight a few civil libertarian brush fires and go on about our private work.

However, examination of the issues surrounding these government actions revealed that we were dealing with the symptoms of a much larger malady, the collision between Society and Cyberspace.

We have concluded that a cure can lie only in bringing civilization to Cyberspace. Unless a successful effort is made to render that harsh and mysterious terrain suitable for ordinary inhabitants, friction between the two worlds will worsen. Constitutional protections, indeed the perceived legitimacy of representative government itself, might gradually disappear.

We could not allow this to happen unchallenged, and so arises the

Electronic Frontier Foundation. In addition to our legal interventions on behalf of those whose rights are threatened, we will:

- Engage in and support efforts to educate both the general public and policymakers about the opportunities and challenges posed by developments in computing and telecommunications.
- Encourage communication between the developers of technology, government, corporate officials, and the general public in which we might define the appropriate metaphors and legal concepts for life in Cyberspace.
- And, finally, foster the development of new tools which will endow non-technical users with full and easy access to computer-based telecommunications.

One of us, Mitch Kapor, had already been a vocal advocate of more accessible software design and had given considerable thought to some of the challenges we now intend to meet.

The other, John Perry Barlow, is a relative newcomer to the world of computing (though not to the world of politics) and is therefore well-equipped to act as an emissary between the magicians of technology and the wary populace who must incorporate this magic into their daily lives.

While we expect the Electronic Frontier Foundation to be a creation of some longevity, we hope to avoid the sclerosis which organizations usually develop in their efforts to exist over time. For this reason we will endeavor to remain light and flexible, marshalling intellectual and financial resources to meet specific purposes rather than finding purposes to match our resources. As is appropriate, we will communicate between ourselves and with our constituents largely over the electronic Net, trusting self-distribution and self-organization to a much greater extent than would be possible for a more traditional organization.

We readily admit that we have our work cut out for us. However, we are greatly encouraged by the overwhelming and positive response which we have received so far. We hope the Electronic Frontier Foundation can function as a focal point for the many people of good will who wish to settle in a future as abundant and free as the present.

The Electronic Frontier Foundation
One Cambridge Center, Suite 300
Cambridge, MA 02142

(617) 577-1385
eff@well.sf.ca.us

Complaint in SJ Games v. Secret Service

Text of the original complaint in Steve Jackson Games vs. U.S. Secret Service, as filed in U.S. Federal Court on May 1, 1991.
Yes, there do seem to be two Roman Numeral III sections. Fnord.

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION
STEVE JACKSON GAMES INCORPORATED, STEVE JACKSON, ELIZABETH McCOY, WALTER MILLIKEN, and STEFFAN O'SULLIVAN, Plaintiffs,
v.UNITED STATES SECRET SERVICE, UNITED STATES OF AMERICA, WILLIAM J. COOK, TIMOTHY M. FOLEY, BARBARA GOLDEN, and HENRY M. KLUEPFEL, Defendants.

COMPLAINT AND DEMAND FOR JURY TRIAL
I. INTRODUCTION AND SUMMARY

This is a civil action for damages to redress violations of the Privacy Protection Act of 1980, 42 U.S.C. 2000aa et seq; the Electronic Communications Privacy Act, as amended, 18 U.S.C. 2510 et seq and 2701 et seq; and the First and Fourth Amendments to the United States Constitution.

Plaintiffs are Steve Jackson Games Incorporated ("SJG"), an award-winning publisher of books, magazines, and games; its president and sole owner Steve Jackson; and three other users of an electronic bulletin board system operated by SJG.

Defendants are the United States Secret Service, the United States of America, an Assistant United States Attorney, Secret Service agents, and a private individual who acted at the direction of these federal officers and agents and under color of federal authority.

Although neither Steve Jackson nor SJG was a target of any criminal investigation, defendants caused a general search of the business premises of SJG and the wholesale seizure, retention, and conversion of computer hardware and software and all data and communications stored there. Defendants seized and retained work product and documentary materials relating to SJG books, games, and magazines, thereby imposing a prior restraint on the publication of such materials. Defendants also seized and retained an entire electronic bulletin board system, including all computer hardware and software used to operate the system and all data and communications stored on the system, causing a prior restraint on the operation of the system. Defendants also seized and retained computer hardware and software, proprietary information, records, and communications used by SJG in the ordinary course of operating its publishing business.

The search of this reputable publishing business and resulting seizures constituted a blatant violation of clearly established law. The search and seizure violated the Privacy Protection Act of 1980, which strictly prohibits law enforcement officers from using search and seizure procedures to obtain work product or documentary materials from a publisher, except in

narrow circumstances not applicable here. The seizure and retention of SJG's work product and bulletin board system, as well as the seizure and retention of the computers used to prepare SJGpublications and to operate the bulletin board system, violated theFirst Amendment. The search and seizure, which encompassed proprietary business information and private electronic communications as well as materials protected by the First Amendment, also violated the Fourth Amendment. Defendants conducted an unconstitutional general search pursuant to a facially invalid, general warrant. The warrant was issued without probable cause to believe that any evidence of criminal activity would be found at SJG and was issued on the basis of false and misleading information supplied by the defendants. Defendants also invaded plaintiffs' privacy by seizing and intercepting the plaintiffs' private electronic communications in violation of the Electronic Communications Privacy Act.

Defendants' wrongful and unlawful conduct amounted to an assault by the government on the plaintiffs, depriving them of their property, their privacy, their First Amendment rights and inflicting humiliation and great emotional distress upon them.

II. DEFINITIONS

When used in this complaint, the following words and phrases have the following meanings:

Computer Hardware: Computer hardware consists of the mechanical, magnetic, electronic, and electrical devices making up a computer system, such as the central processing unit, computer storage devices (disk drives, hard disks, floppy disks), keyboard, monitor, and printing devices.

Computer Software: Computer software consists of computer programs and related instructions and documentation.

Computer Program: A computer program is a set of instructions that, when executed on a computer, cause the computer to process data.

Source Code: Source code is a set of instructions written in computer programming language readable by humans. Source code must be "compiled," "assembled," or "interpreted" with the use of a computer program before it is executable by a computer.

Text File: A computer file is a collection of data treated as a unit by a computer. A text file is a memorandum, letter, or any other alphanumeric text treated as a unit by a computer. A text file can be retrieved from storage and viewed on a computer monitor, printed on paper by a printer compatible with the computer storing the data, or transmitted to another computer.

Modem: A modem, or modulator-demodulator, is an electronic device that makes possible the transmission of data to or from a computer over communications channels, including telephone lines.

Electronic mail: Electronic mail (e-mail) is a data communication transmitted between users of a computer system or network. E-mail is addressed to one or more accounts on a computer system assigned to specific users and is typically stored on the system computer until read and deleted by the addressee. The privacy of electronic mail is typically secured by means of a password, so that only individuals with knowledge of the account's password

can obtain access to mail sent to that account.

Electronic Bulletin Board System (BBS): A BBS is a computerized conferencing system that permits communication and association between and among its users. A system operator ("sysop") manages the BBS on a computer system that is equipped with appropriate hardware and software to store text files and communications and make them accessible to users. Users of the BBS gain access to the system using their own computers and modems and normal telephone lines.

A BBS is similar to a traditional bulletin board in that it allows users to transmit and "post" information readable by other users. Common features of a BBS include:

(1) Conferences in which users engage in an ongoing exchange of information and ideas. Conferences can be limited to a specific group of users, creating an expectation of privacy, or open to the general public.

(2) Archives containing electronically stored text files accessible to users;

(3) Electronic mail service, in which the host computer facilitates the delivery, receipt, and storage of electronic mail sent between users.

Bulletin board systems may be maintained as private systems or permit access to the general public. They range in size from small systems operated by individuals using personal computers in their homes, to medium-sized systemsoperated by groups or commercial organizations, to world-wide networks of interconnected computers. The subject matter and number of topics discussed on a BBS are limited only by the choices of the system's operators and users. Industry estimates indicate that well over a million people in the United States use bulletin board systems.

III. PARTIES

1. Plaintiff SJG is a corporation duly organized and existing under the laws of the State of Texas. At all relevant times, SJG was engaged in the business of publishing adventure games and related books and magazines. Its place of business is 2700-A Metcalfe Road, Austin, Texas.

2. Plaintiff Steve Jackson ("Jackson"), the president and sole owner of SJG, is an adult resident of the State of Texas.

3. Plaintiffs Elizabeth McCoy, Walter Milliken, and Steffan O'Sullivan are adult residents of the State of New Hampshire. At all relevant times, they were users of the electronic bulletin board system provided and operated by SJG and known as the "Illuminati Bulletin Board System" ("Illuminati BBS").

4. The United States Secret Service, an agency within the Treasury Department, and the United States of America sued in Counts I, IV, and V.

5. Defendant William J. Cook ("Cook") is an adult resident of the State of Illinois. At all relevant times,Cook was employed as an Assistant United States Attorney assigned to the United States Attorney's office in Chicago, Illinois. Cook is sued in Counts II-V.

6. Defendant Timothy M. Foley ("Foley") is an adult resident of the State of Illinois. At all relevant times, Foley was employed as a Special Agent of the United States Secret Service, assigned to the office of the United States Secret Service in Chicago, Illinois. At all relevant times, Foley was an attorney licensed to practice law in the State of Illinois. Foley

is sued in Counts II-V.

7. Defendant Barbara Golden ("Golden") is an adult resident of the State of Illinois. At all relevant times, Golden was employed as a Special Agent of the United States Secret Service assigned to the Computer Fraud Section of the United States Secret Service in Chicago, Illinois.

8. Defendant Henry M. Kluepfel ("Kluepfel") is an adult resident of the state of New Jersey. At all relevant times, Kluepfel was employed by Bell Communications Research as a district manager. Kluepfel is sued in Counts II-V.

III. JURISDICTION AND VENUE

9. This Court's jurisdiction is invoked pursuant to 28 U.S.C. 1331 and 42 U.S.C. 2000aa-6(h). Federal question jurisdiction is proper because this is a civil action authorized and instituted pursuant to the First and Fourth Amendments to the United States Constitution, 42 U.S.C. 2000aa-6(a) and 6(h), and 18 U.S.C. 2707 and 2520.

10. Venue in the Western District of Texas is proper under 28 U.S.C. 1391(b), because a substantial part of the events or omissions giving rise to the claims occurred within this District.

IV. STATEMENT OF CLAIMS

FACTUAL BACKGROUND

Steve Jackson Games

11. SJG, established in 1980 and incorporated in 1984, is a publisher of books, magazines, and adventure games.

(a) SJG books and games create imaginary worlds whose settings range from prehistoric to futuristic times and whose form encompass various literary genres.

(b) The magazines published by SJG contain news, information, and entertainment relating to the adventure game industry and related literary genres.

12. SJG games and publications are carried by wholesale distributors throughout the United States and abroad.

13. SJG books are sold by national retail chain stores including B. Dalton, Bookstop, and Waldenbooks.

14. Each year from 1981 through 1989, and again in 1991, SJG board games, game books, and/or magazines have been nominated for and/or received the Origins Award. The Origins Award, administered by the Game Manufacturers' Association, is the adventure game industry's most prestigious award.

15. SJG is not, and has never been, in the business of selling computer games, computer programs, or other computer products.

16. On March 1, 1990, SJG had 17 employees.

Steve Jackson Games Computer Use

17. At all relevant times, SJG relied upon computers for many aspects of its business, including but not limited to the following uses: (a) Like other publishers of books or magazines, and like a newspaper publisher, SJG used computers to compose, store, and prepare for publication the text of its

books, magazines, and games.

(b) SJG stored notes, source materials, and other work product and documentary materials relating to SJG publications on its computers.

(c) Like many businesses, SJG used computers to create and store business records including, but not limited to, correspondence, contracts, address directories, budgetary and payroll information, personnel information, and correspondence.

18. Since 1986, SJG has used a computer to operate an electronic bulletin board system (BBS) dedicated to communication of information about adventure games, the game industry, related literary genres, and to association among individuals who share these interests.

(a) The BBS was named "Illuminati," after the company's award-winning board
game.

(b) At all relevant times, the Illuminati BBS was operated by means of a computer located on the business premises of SJG. The computer used to run the Illuminati BBS (hereafter the "Illuminati computer") was connected to the telephone number 512-447-4449. Users obtained access to communications and information stored on the Illuminati BBS from their own computers via telephone lines.

(c) The Illuminati BBS provided a forum for communication and association among its users, which included SJG employees, customers, retailers, writers, artists, competitors, writers of science fiction and fantasy, and others with an interest in the adventure game industry or related literary genres.

(d) SJG, Jackson, and SJG employees also used the Illuminati BBS in the course of business to communicate with customers, retailers, writers, and artists; to provide customer service; to obtain feedback on games and new game ideas; to obtain general marketing information; to advertise its games and publications, and to establish good will and a sense of community with others who shared common interests.

(e) As of February 1990, the Illuminati BBS had over 300 users residing throughout the United States and abroad.

(f) At all relevant times, plaintiffs SJG, Jackson, McCoy, Milliken, and O'Sullivan were active users of the Illuminati BBS.

(g) Each user account was assigned a password to secure the privacy of the account.

(h) The Illuminati BBS gave users access to general files of electronically stored information. General files included, but were not limited to, text files containing articles on adventure games and game-related humor, including articles published in SJG magazines and articles contributed by users of the BBS, and text files containing game rules. These general files were stored on the Illuminati computer at SJG.

(i) The Illuminati BBS provided several public conferences, in which users of the BBS could post information readable by other users and read information posted by others. The discussions in the public conferences focused on SJG products, publications and related literary genres. All communications transmitted to these conferences were stored in the Illuminati

computer at SJG.

(j) SJG informed users of the Illuminati BBS that "any opinions expressed on the BBS, unless specifically identified as the opinions or policy of Steve Jackson Games Incorporated, are only those of the person posting them. SJ Games will do its best to remove any false, harmful or otherwise obnoxious material posted, but accepts no responsibility for material placed on this board without its knowledge.

(k) The Illuminati BBS also provided private conferences that were accessible only to certain users authorized by SJG and not to the general public. All communications transmitted to these conferences were stored in the Illuminati computer at SJG.

(l) The Illuminati BBS provided a private electronic mail (e-mail) service, which permitted the transmission of private communications between users on the system as follows:

(i) E-mail transmitted to an account on the Illuminati BBS was stored on the BBS computer until deleted by the addressee.

(ii) The privacy of e-mail was secured by the use of passwords.

(iii) The privacy of e-mail was also secured by computer software that prevented the system operator from reading e-mail inadvertently.

(iv) The privacy of e-mail was also secured by SJG policy. SJG informed users of the Illuminati BBS that "[e]lectronic mail is private." (v) As a matter of policy, practice, and customer expectations, SJG did not read e-mail addressed to Illuminati users other than SJG.

(vi) At all relevant times, all plaintiffs used the e-mail service on the Illuminati BBS.

(vii) On March 1, 1990, the Illuminati computer contained stored e-mail sent to or from each of the plaintiffs.The Illegal Warrant and Application

19. On February 28, 1990, defendant Foley filed an application with this Court, for a warrant authorizing the search of the business premises of SJG and seizure of "[c]omputer hardware (including, but not limited to, central processing unit(s), monitors, memory devices, modem(s), programming equipment, communication equipment, disks, and prints) and computer software (including, but not limited to, memory disks, floppy disks, storage media) and written material and documents relating to the use of the computer system (including networking access files), documentation relating to the attacking of computers and advertising the results of computer attacks (including telephone numbers and location information), and financial documents and licensing documentation relative to the computer programs and equipment at the business known as Steve Jackson Games which constitute evidence, instrumentalities and fruits of federal crimes, including interstate transportation of stolen property (18 USC 2314) and interstate transportation of computer access information (18 USC 1030(a)(6)). This warrant is for the seizure of the above described computer and computer data and for the authorization to read information stored and contained on the above described computer and computer data."A copy of the application and supporting affidavit of defendant Foley (hereafter "Foley affidavit") are attached as Exhibit "A" and incorporated herein by reference.

20. The search warrant was sought as part of an investigation being

conducted jointly by defendant Cook and the United States Attorney's office in Chicago; defendants Foley, Golden, and the Chicago field office of the United States Secret Service; and defendant Kluepfel.

21. On information and belief, neither SJG nor Jackson nor any of the plaintiffs were targets of this investigation.

22. The Foley affidavit was based on the investigation of defendant Foley and on information and investigative assistance provided to him by others, including defendants Golden and Kluepfel and unnamed agents of the United States Secret Service. Foley Affidavit para. 3.

23. The Foley affidavit alleged that defendant Kluepfel had partipated in the execution of numerous federal and state search warrants. Id.

24. On information and belief, Defendant Cook participated in the drafting, review, and submission of the warrant application and supporting affidavit to this Court.

25. The warrant application and supporting affidavit were placed under seal on motion of the United States.

26. On February 28, 1990, based on the Foley affidavit, a United States Magistrate for the Western District of Texas granted defendant Foley's warrant application and issued awarrant authorizing the requested search and seizure described in paragraph 19 above. A copy of the search warrant is attached as Exhibit B.

27. The warrant was facially invalid for the following reasons:

(a) It was a general warrant that failed to describe the place to be searched with particularity.

(b) It was a general warrant that failed to describe things to be seized with particularity.

(c) It swept within its scope handwritten, typed, printed, and electronically stored communications, work product, documents, and publications protected by the First Amendment.

(d) It swept within its scope SJG proprietary information and business records relating to activities protected by the First Amendment.

(e) It swept within its scope a BBS that was a forum for speech and association protected by the First Amendment.

(f) It swept within its scope computer hardware and software that were used by SJG to publish books, magazines, and games.

(g) It swept within its scope computer hardware and software used by SJG to operate a BBS.

28. The warrant was also invalid in that it authorized the seizure of work product and documentary materials from a publisher "reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce," which is generally prohibited by 42 U.S.C. 2000aa(a) and (b), without showing the existence of any of the narrow statutory exceptions in which such a search and seizure is permitted. Specifically, the Foley affidavit did not establish the existence of any of the following circumstances: (a) The Foley affidavit did not establish probable cause to believe that SJG, or any employee in possession of work product materials at SJG, had committed or was committing a criminal offense to which such materials related.

(b) The Foley affidavit did not establish probable cause to believe that SJG or any employee of SJG in possession of work product materials at SJG, had committed or was committing a criminal offense to which such materials related consisting of other than the receipt possession, communication, or withholding of such materials or the information contained therein.

(c) The Foley affidavit did not establish probable cause to believe that SJG, or any employee of SJG in possession of work product materials at SJG, had committed or was committing a criminal offense consisting of the receipt, possession, or communication of information relating to the national defense, classified information, or restricted data under the provisions of 18 U.S.C. 793, 794, 797, or 798 or 50 U.S.C. 783.

(d) The Foley affidavit did not establish reason to believe that immediate seizure of work product materials from SJG was necessary to prevent the death of, or serious bodily injury to, a human being.

(e) The Foley affidavit did not establish probable cause to believe that SJG, or any employee of SJG in possession of documentary materials at SJG, had committed or was committing a criminal offense to which the materials related.

(f) The Foley affidavit did not establish probable cause to believe that SJG, or any employee of SJG in possession of documentary materials at SJG had committed or was committing a criminal offense to which the materials related consisting of other than the receipt, possession, communication, or withholding of such materials or the information contained therein.

(g) The Foley affidavit did not establish probable cause to believe that SJG, or any employee of SJG in possession of documentary materials at SJG, had committed or was committing an offense consisting of the receipt, possession, or communication of information relating to the national defense, classified information, or restricted data under the provisions of 18 U.S.C. 793, 794, 797, or 798 or 50 U.S.C. 783.

(h) The Foley affidavit did not establish reason to believe that the immediate seizure of such documentary materials was necessary to prevent the death of, or serious bodily injury to, a human being.

(i) The Foley affidavit did not establish reason to believe that the giving of notice pursuant to a subpoena duces tecum would result in the destruction, alteration, or concealment of such documentary materials.

(j) The Foley affidavit did not establish that such documentary materials had not been produced in response to a court order directing compliance with a subpoena duces tecum and that all appellate remedies had been exhausted or that there was reason to believe that the delay in an investigation or trial occasioned by further proceedings relating to the subpoena would threaten the interests of justice.

29. The warrant was invalid because the warrant application and supporting affidavit of defendant Foley did not establish probable cause to believe that the business premises of SJG was a place where evidence of criminal activity would be found, in that:

(a) The Foley affidavit did not allege that evidence of criminal activity would be found at SJG. Rather, the affidavit alleged that "E911 source code and text file" and a "decryption software program" would be "found

in the computers located at 1517G Summerstone, Austin, Texas, or at 2700-A Metcalfe Road, Austin, Texas [SJG], or at 3524 Graystone #192, or in the computers at each of those locations." Foley Affidavit para. 30 (emphasis added).

(b) The Foley affidavit did not establish probable cause to believe that E911 source code would be found at the business premises of SJG.

(c) The Foley affidavit did not establish probable cause to believe that an E911 text file would be found at the business premises of SJG.

(d) The Foley affidavit did not establish probable cause to believe that a decryption software program would be found at the business premises of SJG.

30. Even assuming, arguendo, that the warrant affidavit demonstrated probable cause to believe that "E911 source code and text file" and a "password decryption program" would be found at the business premises of SJG, the warrant was still invalid because its description of items to be seized was broader than any probable cause shown, in that:

(a) The warrant authorized the seizure of computer hardware, software, and documentation that did not constitute evidence, instrumentalities, or fruits of criminal activity;

(b) The warrant authorized the seizure and reading of electronically stored data, including publications, work product, proprietary information, business records, personnel records, and correspondence, that did not constitute evidence, instrumentalities, or fruits of criminal activity;

(c) The warrant authorized the seizure and reading of electronically stored communications that were not accessible to the public, including private electronic mail, and that did not constitute evidence, instrumentalities, or fruits of criminal activity.

31. The warrant is invalid because there is nothing in the Foley affidavit to show that the information provided by defendant Kluepfel regarding the BBS at SJG was not stale.

32. The warrant was invalid because the Foley affidavit was materially false and misleading, and because defendants submitted it knowing it was false and misleading or with reckless disregard for the truth, as set forth in paragraphs 33-40 below.

33. The Foley affidavit did not inform the Magistrate that SJG was a publisher of games, books, and magazines, engaged in the business of preparing such materials for public dissemination in or affecting interstate commerce;

(a) This omission was material;

(b) Defendants omitted this material information from the warrant application knowingly or with reckless disregard for the truth or falsity of the application.

34. The Foley affidavit did not inform the Magistrate that SJG used computers to compose and prepare publications for public dissemination;

(a) This omission was material;

(b) Defendants omitted this material information from the warrant application knowingly or with reckless disregard for the truth or falsity of the application.

35. The Foley affidavit did not inform the Magistrate that the computer at SJG used to operate the BBS contained electronically stored texts,

work product, documentary materials, and communications stored for the purpose of public dissemination in or affecting interstate commerce; (a) This omission was material;

(b) Defendants omitted this material information from the warrant application knowingly or with reckless disregard for the truth or falsity of the application.

36. The Foley affidavit did not inform the Magistrate that a computer used to operate the BBS at SJG operated a forum for constitutionally protected speech and association regarding adventure games and related literary genres;

(a) This omission was material;

(b) Defendants omitted this material information from the warrant application knowingly or with reckless disregard for the truth or falsity of the application.

37. The Foley affidavit did not inform the Magistrate that the computer used to operate the BBS at SJG contained stored private electronic communications;

(a) This omission was material;

(b) Defendants omitted this material information from the warrant application knowingly or with reckless disregard for the truth or falsity of the application.

38. The Foley affidavit falsely alleged that the E911 text file was a "program." Foley Affidavit paras. 8, 14, 17;

(a) This false allegation was material;

(b) Defendants made this material false allegation knowingly or with reckless disregard for its truth or falsity;

(c) Defendants Cook and Foley have acknowledged that the E911 text file is not a program.

39. The affidavit of defendant Foley falsely alleges that the information in the E911 text file was "highly proprietary" and "sensitive". Foley Affidavit paras. 13, 14, 22;

(a) This false allegation was material;

(b) Defendants made this material false allegation knowingly or with reckless disregard for its truth or falsity;

(c) Defendant Cook has acknowledged that much of the information in the E911 text file had been disclosed to the public.

40. The affidavit of defendant Foley falsely alleges that the E911 text file was "worth approximately $79,000.00," para. 4, and "engineered at a cost of $79,449.00," para. 14;

(a) This false allegation was material;

(b) Defendants made this material false allegation knowingly or with reckless disregard for its truth or falsity;

(c) Defendant Cook has acknowledged that the value of the nondisclosed information in the E911 text file was less than the $5000.00 jurisdictional minimum for Interstate Transportation of Stolen Property, 18 U.S.C. 2314.

41. Reasonable persons in defendants' position would have known that the warrant was invalid for the reasons given in paragraphs 27-40 and would not have requested or relied on the warrant. The Search and Seizure:

42. Nevertheless, on March 1, 1990, defendant Golden, other agents of the United States Secret Service, and others acting in concert with them,

conducted a general search of the SJG office and warehouse.

43. The searching officers prevented SJG employees from entering their workplace or conducting any business from 8:00 a.m. until after 1:00 p.m. on March 1, 1990.

44. The agents seized computer hardware and related documentation, including, but not limited to, the following:

(a) three central processing units;

(b) hard drives;

(c) hundreds of disks;

(d 2 monitors;

(e) 3 keyboards;

(f) 3 modems;

(g) a printer;

(h) electrical equipment including, but not limited to, extension cords, cables, and adapters;

(i) screws, nuts, and other small parts.

45. The agents seized all computer hardware, computer software, and supporting documentation used by SJG to run the Illuminati BBS, thereby causing the following to occur:

(a) the seizure of all programs, text files, and public communications stored on the BBS computer;

(b) the seizure of all private electronic communications stored on the system, including electronic mail;

(c) preventing plaintiffs from operating and using the BBS.

46. The agents seized computer software and supporting documentation that SJG used in the ordinary course of its business including, but not limited to, word processing software.

47. The defendants seized all data stored on the seized SJG computers and disks, including, but not limited to, the following:

(a) SJG work product, including drafts of forthcoming publications and games;

(b) Communications from customers and others regarding SJG's games, books, and magazines;

(c) SJG financial projections;

(d) SJG contracts;

(e) SJG correspondence;

(f) SJG editorial manual, containing instructions and procedures for writers and editors;

(g) SJG address directories, contacts lists, and employee information, including the home telephone numbers of SJG employees.

48. The defendants seized all current drafts - both electronically stored copies and printed ("hard") copies - of the book GURPS Cyberpunk, which was scheduled to go to the printer later that week. (a) GURPS Cyberpunk was part of a series of fantasy roleplaying game books published by SJG called the Generic Universal Roleplaying System.

(b) The term "Cyberpunk" refers to a science fiction literary genre which became popular in the 1980s. The Cyberpunk genre is characterized by the fictional interaction of humans with technology and the fictional struggle for

power between individuals, corporations, and government. One of the most popular examples of the Cyberpunk genre is William Gibson's critically acclaimed science fiction novel Neuromancer, which was published in 1984.

(c) GURPS Cyberpunk is a fantasy roleplaying game book of the Cyberpunk genre.

(d) SJG eventually published the book GURPS Cyberpunk in 1990.

(e) The book has been distributed both nationally and internationally.

(f) To date SJG has sold over 16,000 copies of the book.

(g) The book has been nominated for an Origins Award for Best Roleplaying Supplement.

(h) The book is used in at least one college literature course as an example of the Cyberpunk genre.

49. The search and seizure exceeded the scope of the warrant, in that the searching officers seized computer hardware, computer software, data, documentation, work product, and correspondence that did not constitute evidence, instrumentalities or fruits of any crime.

50. The search was conducted in a reckless and destructive fashion, in that the searching officers caused damage to SJG property and left the SJG office and warehouse in disarray.Post-seizure Retention of Property

51. Plaintiffs Jackson and SJG put defendants on immediate notice that they had seized the current drafts of the about-to-be-published book GURPS Cyberpunk and the computer hardware and software necessary to operate a BBS and requested immediate return of these materials.

52. SJG and Jackson made diligent efforts to obtain the return of the seized equipment and data, including but not limited to, retention of legal counsel, numerous telephone calls to defendants Cook and Foley by Jackson and SJG counsel, a trip to the Austin Secret Service office, and correspondence with defendants Cook and Foley and with other federal officials.

53. On March 2, 1990, Jackson went to the Austin office of the Secret Service in an unsuccessful attempt to obtain the return of seized documents and computer data, including the drafts of the forthcoming book GURPS Cyberpunk and the software and files stored on the Illuminati BBS.

54. On March 2, 1990, the Secret Service refused to provide Jackson with the files containing current drafts of GURPS Cyberpunk, one agent calling the book a "handbook for computer crime."

55. On March 2, 1990, the Secret Service also refused to return copies of the software used to run the Illuminati BBS and copies of any of the data or communications stored on the BBS.

56. In the months following the seizure, defendant Cook repeatedly gave Jackson and his counsel false assurances that the property of SJG would be returned within days.

57. In May of 1990, Jackson wrote to Senators Philip Gramm and Lloyd Bentsen and Congressman J. J. Pickle, regarding the search and seizure conducted at SJG and requesting their assistance in obtaining the return of SJG property.

58. On June 21, 1990, the Secret Service returned most, but not all, of the computer equipment that had been seized from SJG over three months earlier.

59. The Secret Service did not return some of SJG's hardware and data.

60. The Secret Service did not return any of the printed drafts of GURPS Cyberpunk.

61. In July 3, 1990, letters to Senator Bentsen and Congressman J. J. Pickle, Robert R. Snow of the United States Secret Service falsely stated that all of the items seized from SJG had been returned to Jackson.

62. In his July 16, 1990, letter to Senator Gramm, Bryce L. Harlow of the United States Department of Treasury falsely stated that all of the items seized from SJG had been returned to Jackson.

63. Through counsel, SJG wrote to defendant Foley on July 13, 1990, requesting, inter alia, a copy of the application for the search warrant and return of the property the government had not returned. A copy of this letter was mailed to Defendant Cook. Though the letter requested a response by August 1, 1990, neither defendant responded.

64. Through counsel, plaintiff SJG again wrote to defendant Cook on August 8, 1990, requesting, inter alia, a copy of the application for the search warrant and return of the property the government had not returned. Copies of this letter were sent to other Assistant United States Attorneys in Chicago, namely Thomas Durkin, Dean Polales, and Michael Shepard.

65. Defendant Cook responded to this request with an unsigned letter dated August 10, 1990. The letter enclosed a number of documents that had not previously been returned to SJG. The letter further stated that "the application for the search warrant is under seal with the United States District Court in Texas since it contains information relating to an ongoing federal investigation."

66. On September 17, 1990, the warrant affidavit was unsealed by the United States Magistrate for the Western District of Texas on the motion of the United States Attorney for the Northern District of Illinois.

67. The United States Attorney's office did not provide Jackson, SJG or their counsel with notice of its motion to unseal the warrant affidavit or of this Court's order granting its motion.Prior Restraint on Publication and Other Damages:

68. Defendants' seizure and retention of the computer hardware and software used to operate the Illuminati BBS prevented and interfered with plaintiffs' operation and use of the Illuminati BBS, including the following:

(a) In an attempt to minimize the damage caused by defendants' conduct, SJG purchased replacement computer hardware and software to operate the Illuminati BBS;

(b) As a result of defendants' conduct, SJG was unable to operate or use the Illuminati BBS for over a month;

(c) As a result of defendants' conduct, plaintiffs were deprived of the use of the Illuminati BBS for over a month;

(d) Defendants seized and intercepted electronic mail in which plaintiffs had a reasonable expectation of privacy;

(e) Users of the BBS were substantially chilled in their exercise of their constitutionally protected rights of freedom of speech and association;

(f) Some of the data previously available to users of the Illuminati BBS was lost or destroyed.

69. Defendants' conduct caused a prior restraint of the publication of the book GURPS Cyberpunk, in that:

(a) On March 1, 1990, the book GURPS Cyberpunk was nearly completed and scheduled to be sent to the printer the following week;

(b) On March 1, 1990, defendants caused the illegal seizure of all of the current drafts of GURPS Cyberpunk, including both printed drafts and electronically stored drafts.

(c) On March 1, 1990, Defendants caused the illegal seizure of electronic communications stored on the Illuminati BBS containing comments on GURPS Cyberpunk.

(d) Defendants unreasonably refused for weeks to return the electronically stored drafts of GURPS Cyberpunk.

(e) Defendants have not yet returned the printed drafts of GURPS Cyberpunk.

(f) Defendants refused to return electronically stored comments regarding GURPS Cyberpunk for over three months.

(g) By their conduct, defendants prevented SJG from delivering GURPS Cyberpunk to the printer on schedule, and caused SJG to miss its publication deadline.

(h) As a result of defendants' conduct, and in an attempt to minimize damages, SJG and its employees reconstructed and rewrote GURPS Cyberpunk from older drafts.

(i) As a result of defendants' conduct, the publication of GURPS Cyberpunk was delayed for six weeks.

70. Defendants' conduct caused substantial delay in the publication and delivery of other SJG publications.

71. As a result of defendants' conduct, SJG suffered substantial financial harm including, but not limited to, lost sales, lost credit lines, interest on loans, late payment penalties, and attorney's fees and costs.

72. As a result of defendants' conduct, SJG was forced to lay off 8 of its 17 employees.

73. As a result of defendants' conduct, SJG suffered damage to its business reputation.

74. As a result of defendants' conduct, SJG has suffered loss of, damage to, and conversion of computer equipment and data, including, but not limited to, the following:

(a) loss of and damage to computer hardware;

(b) loss and destruction of seized data;

75. Defendants have retained copies of data seized from SJG.

76. As a result of defendants' conduct, plaintiff Steve Jackson has suffered additional harm including, but not limited to, lost income, damage to professional reputation, humiliation, invasion of privacy, deprivation of constitutional rights, and emotional distress.

77. As a result of defendants' conduct, plaintiffs McCoy, Milliken, and O'Sullivan have suffered additional harm including, but not limited to, damages resulting from the seizure of their private electronic mail and the interference with, and temporary shut down of, the Illuminati forum for speech and association, deprivation of their constitutional rights, invasion of their privacy, and emotional distress.

COUNT I:

PRIVACY PROTECTION ACT OF 1980,
42 U.S.C. 2000aa et seq
Against the United States Secret Service and the United States of America

78. The allegations in paragraphs 1-77 are incorporated herein by reference.

79. At all relevant times, SJG and its employees were persons "reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce" within the meaning of 42 U.S.C. 2000aa(a) and (b).

80. At all relevant times, SJG and its employees possessed work product and documentary materials in connection with a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce.

81. Defendants caused the submission of an application for a warrant to search the business premises of SJG and to seize work product materials therefrom, in violation of 42 U.S.C. 2000aa, in that:

(a) The Foley affidavit did not inform the Magistrate that SJG and its employees were persons "reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce" within the meaning of 42 U.S.C. 2000aa(a) and (b).

(b) The Foley affidavit did not inform the Magistrate that SJG and its employees possessed work product materials and documentary materials in connection with a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce.

(c) The Foley affidavit did not establish that any of the exceptions to the statutory prohibition of searches and seizures set out in 42 U.S.C. 2000aa(a) and (b) existed.

82. Defendants caused the March 1, 1990, search of the business premises of SJG and seizure of work product and documentary materials therefrom in violation of 42 U.S.C. 2000aa et seq.

83. Defendants Cook, Foley, and Golden were federal officers and employees acting within the scope or under color of federal office or employment.

84. Defendant Kluepfel acted in concert with federal agents under color of federal office.

85. Plaintiffs SJG, Jackson, McCoy, Milliken, and O'Sullivan are all persons aggrieved by defendants' conduct, having suffered damages, attorney's fees, and costs, as a direct result of defendants' conduct.

86. The United States of American and the United States Secret Service are liable to plaintiffs for damages, attorney's fees and costs caused by defendants' conduct.

COUNT II:
FIRST AMENDMENT
Against Defendants Cook, Foley, Golden & Kluepfel

87. The allegations in paragraphs 1-86 are incorporated herein by

reference.

88. Defendants violated plaintiffs' rights to freedom of speech, freedom of the press, and freedom of association as guaranteed by the First Amendment, in that:

(a) At all relevant times SJG was a publisher of books, magazines, and games protected by the First Amendment;

(b) At all relevant times SJG was the operator of a BBS that was a forum for speech and association protected by the First Amendment;

(c) At all relevant times, plaintiffs SJG, Jackson, McCoy, Milliken, and O'Sullivan used the Illuminati BBS for speech and association protected by the First Amendment;

(d) At all relevant times, plaintiff SJG used computers to publish books, magazines, and games and to operate the Illuminati BBS;

(e) The search, seizure, and retention of SJG work product - both printed and electronically stored - caused a prior restraint on SJG publications in violation of plaintiffs' First Amendment rights of freedom of speech and of the press;

(f) The search and seizure of the Illuminati BBS constituted a prior restraint on plaintiffs' exercise of their First Amendment rights of freedom of speech, of the press, and of association;

(g) The seizure and retention of computer hardware and software used by SJG to publish books, magazines, and games violated plaintiffs' rights to freedom of speech and of the press;

(h) The seizure and retention of computer hardware and software used by SJG to operate a BBS violated plaintiffs' First Amendment rights to freedom of speech, of the press, and of association.

89. Defendants knew or reasonably should have known that their conduct violated plaintiffs' clearly established First Amendment rights of freedom of speech, freedom of the press, and freedom of association.

90. Defendants acted with intent to violate, or with reckless indifference to, plaintiffs' clearly established First Amendment rights to freedom of speech, freedom of the press, and freedom of association.

91. Defendants Cook, Foley, and Golden acted as federal agents and under color of federal law.

92. Defendant Kluepfel acted in concert with the federal defendants under color of federal law.

93. As a direct result of the defendants' conduct, plaintiffs have suffered damages.

COUNT III:
FOURTH AMENDMENT
Against Defendants Cook, Foley, Golden, and Kluepfel

94. The allegations in paragraphs 1-93 are incorporated herein by reference.

95. The defendants, by their actions, violated plaintiffs' clearly established right to be free from unreasonable searches and seizures as guaranteed by the Fourth Amendment to the United States Constitution, in that:

(a) Plaintiffs SJG and Jackson had a reasonable expectation of privacy in the business premises of SJG and in all SJG work product, SJG records, and

SJG documents kept there, including in all data stored in the computers at SJG;

(b) All plaintiffs had a reasonable expectation of privacy in private electronic communications stored on the Illuminati BBS at SJG;

(c) The search and seizure at SJG games was a general search;

(d) The search and seizure at SJG was not authorized by a valid warrant particularly describing the place to be searched and the things to be seized;

(e) The search and seizure at SJG was conducted without probable cause to believe that evidence of criminal activity would be found at SJG;

(f) The search and seizure at SJG was based on information that was not shown to be current;

(g) Defendants' warrant application was materially false and misleading, and was submitted by defendants with knowledge of its false and misleading nature or with reckless disregard for its truth or falsity.

96. The defendants knew, or reasonably should have known, that their conduct violated plaintiffs' clearly established constitutional right to be free from unreasonable searches and seizures.

97. The defendants acted with intent to violate, or with reckless indifference to, plaintiffs' clearly established Fourth Amendment rights.

98. Defendants Cook, Foley, and Golden acted as federal agents and under color of federal law.

99. Defendant Kluepfel acted in concert with the federal defendants and under color of federal law.

100. As a direct result of the defendants' actions, plaintiffs suffered damages, attorney's fees and costs.

COUNT IV:
ELECTRONIC COMMUNICATIONS PRIVACY ACT, 18 U.S.C. 2707
Seizure of Stored Electronic Communications Against All Defendants

101. The allegations in paragraphs 1-100 are incorporated herein by reference.

102. At all times relevant times, plaintiff SJG was the provider of an electronic communication service within the meaning of 18 U.S.C. 2510(15) and 2707.

103. At all relevant times, plaintiffs SJG, Jackson, McCoy, Milliken, and O'Sullivan were subscribers to or customers of the electronic communication service provided by SJG within the meaning of 18 U.S.C. 2510(15) and 2707.

104. At all relevant times, plaintiffs had electronic communications in electronic storage on the communicationservice provided by SJG that were not accessible to the general public.

105. Defendants applied for a warrant to search and seize the computer operating the electronic communication service provided by SJG and all data stored thereon, but failed to inform the Magistrate that the computer contained stored electronic communications that were not accessible to the general public.

106. Defendants, acting without a valid warrant, required SJG to

disclose the contents of electronic communications that were not accessible to the general public and that were in electronic storage for 180 days or less, in violation of 18 U.S.C. 2703(a).

107. Defendants disrupted the normal operations of the communication service operated by SJG without compensation to plaintiffs in violation of 18 U.S.C. 2706(a).

108. Defendants Cook, Foley, and Golden acted as federal agents and under color of federal law.

109. Defendant Kluepfel acted in concert with the federal defendants and under color of federal law.

110. Defendants acted knowingly and intentionally.

111. Defendants did not act in good faith.

112. Plaintiffs were aggrieved by defendants' conduct, and suffered damages, attorney's fees and costs.

COUNT V:
ELECTRONIC COMMUNICATIONS PRIVACY ACT, 18 U.S.C. 2510 et seq.
Interception of Electronic Communications
Against All Defendants

113. The allegations in paragraphs 1-112 are incorporated herein by reference.

114. Defendants intercepted, disclosed, or intentionally used plaintiffs' electronic communications in violation of 18 U.S.C. 2510 et seq and 2520.

115. Defendants intentionally intercepted, endeavored to intercept, or procured others to intercept or endeavor to intercept, plaintiffs' electronic communications in violation of 18 U.S.C. 2511(1)(a).

116. Defendants did not comply with the standards and procedures prescribed in 18 U.S.C. 2518.

117. The warrant application was not authorized by the Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney general, acting Assistant Attorney General, or any Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General, in violation of 18 U.S.C. 2516.

118. Defendants Cook, Foley, and Golden acted as federal agents and under color of federal law.

119. Defendant Kluepfel acted in concert with the federal defendants and under color of federal law.

120. Defendants did not act in good faith.

121. Defendants did not compensate plaintiffs for reasonable expenses incurred by defendants' seizure of the Illuminati BBS, in violation of 18 U.S.C. 2518(4).

122. As a direct result of defendants' conduct, plaintiffs suffered damages, attorney's fees and costs.Prayers for Relief

WHEREFORE, plaintiffs SJG, Jackson, McCoy, Milliken, and O'Sullivan pray that this Court:

1. Assume jurisdiction of this case.

2. Enter judgment against defendants and in favor of plaintiffs.

3. Enter an order requiring defendants to return all property and data

seized from the premises of SJG, and all copies of such data, to SJG.

4. Award plaintiffs damages.

5. Award plaintiffs punitive and liquidated damages.

6. Award plaintiffs all costs incurred in the prosecution of this action, including reasonable attorney's fees.

7. Provide such additional relief as may appear to the Court to be just.

PLAINTIFFS DEMAND A JURY TRIAL ON ALL CLAIMS TRIABLE BY JURY

Dated: May 1, 1991

Respectfully submitted by their attorneys,

Sharon L. Beckman
Harvey A. Silverglate
Andrew Good
SILVERGLATE & GOOD
89 Broad St., 14th floor
Boston, MA 02110
(617) 542-6663
Fax: (617) 451-6971

Eric M. Lieberman
Nicholas E. Poser
Rabinowitz, Boudin, Standard, Krinsky & Lieberman, P.C.
740 Broadway, at Astor Place
New York, NY 10003-9518
(212) 254-1111
Fax: (212) 674-4614

R. James George, Jr.
Graves, Dougherty, Hearon & Moody
2300 NCNB Tower
515 Congress Street
Austin, Texas 78701
(512) 480-5600
Fax: (512) 478-1976

JUDGE'S DECISION IN SJ GAMES VS. SECRET SERVICE

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

STEVE JACKSON GAMES
INCORPORATED, et al.,
Plaintiffs,

v.

UNITED STATES SECRET SERVICE, UNITED STATES OF AMERICA, et al., Defendants

Opinion

I. Facts

The issues remaining at trial in this lawsuit involves the Plaintiffs Steve Jackson Games, Incorporated, Steve Jackson, Elizabeth McCoy, Walter Milliken, and Steffan O'Sullivan's causes of action against the United States Secret Service and the United States of America pursuant to three statutes, "Private Protection Act", 42 U.S.C. 2000aa _et seq_.; "Wire and Electronic Communications Interception and Interception of Oral Communication' Act, 18 U.S.C. 2510, et seq.; and "Stored Wire and Electronic Communications and Transactional Records Access" Act, 18 U.S.C 2701, _et seq_. All other issues and parties have been withdrawn by agreement of these remaining parties.

The individual party plaintiffs are residents of the states of Texas and New Hampshire, and the corporate plaintiff is a Texas corporation with its principal place of business in Austin, Texas.

The Plaintiff Steve Jackson started Steve Jackson Games in 1980 and subsequently incorporated his business. Steve Jackson Games, Incorporated, publishes books, magazines, box games, and related products (F1.) More than 50 percent of the corporation's revenues are derived from its publications. In addition, Steve Jackson Games, Incorporated, beginning in the mid-1980s and continuing through this litigation, operated from one of its computers an electronic bulletin board system called Illuminati. This bulletin board posts information to the inquiring public about Steve Jackson Games' products and activities; provides a medium for receiving and passing on information from the corporation's employees, writers,

customers, and its game enthusiasts; and, finally, affords its users electronic mail whereby, with the use of selected passwords, its users can send and receive electronic mail (E-mail) in both public and private modes. In February of 1990, there were 365 users of the Illuminati bulletin board.

Steve Jackson was both the owner and employee of Steve Jackson Games, Incorporated, and authored many of its publications; he used both Illuminati's public and private programs for electronic mail and his use ranged from business records of the corporation, contracts with his writers, communication with his writers regarding articles which were intended to be published by the corporation, to private communications with his business associates and friends. Elizabeth McCoy's use of the Illuminati bulletin board involved her participation as a game player, her critiques as to the games and publications of the corporation, and her private communications with associates and friends. William Milliken's use of the Illuminati bulletin board was apparently limited to private communicates to associates and friends. Steffan O'Sullivan's use of the Illuminati bulletin board included writings for publication by Steve Jackson Games, Inc., his business dealings with the corporation, and public and private communications with associates and friends.

Importantly, prior to March l, 1990, and at all other times, there has never been any basis for suspicion that any of the Plaintiffs have engaged in any criminal activity, violated any law, or attempted to communicate, publish, or store any illegally obtained information or otherwise provide access to any illegally obtained information or to solicit any information which was to be used illegally.

In October of 1988, Henry Kluepfel, Director of Network Security Technology (an affiliate Bell Company), was advised a sensitive, proprietary computer document of Bell South relating to Bell's "911 program" had been made available to the public on a computer bulletin board in Illinois. Kluepfel reported this information to Bell South and requested instructions, but received no response. In April of 1989, Kluepfel confirmed the 911 Bell document was available on the Illinois computer bulletin board and learned the document was additionally available without any proprietary notice on at least another computer bulletin board and had been or was being published in a computer bulletin board newsletter in edited form. In July of 1989, Kluepfel was finally instructed by Bell South to report the "intrusion of its computer network to the Secret Service and that the document taken was "sensitive" and "proprietary. Kluepfel had previously worked with the Secret Service and was known as an expert and reliable informant on computer "hacking." (F2) Thereafter, Kluepfel met Assistant U. S. Attorney William Cook in Chicago and thereafter communicated with Cook and Secret Service Agent Tim Foley. Agent Foley was in charge of this particular investigation.

Around February 6, l990, Kluepfel learned that the 911 document was available on a computer billboard entitled "Phoenix" which was operated by Loyd Blankenship in Austin, Texas. Kluepfel "downloaded" the document to put in readable form and then advised these facts to the Secret Service. Prior to February 26, 1990, Kluepfel learned that Blankenship not only operated the Phoenix bulletin board, but he was a user of the Illinois bulletin board wherein the 911 document was first disclosed, was an employee of Steve Jackson Games, Inc., and a user of the Steve Jackson Games, Inc.'s bulletin board "Illuminati." Kluepfel's investigation also determined that Blankenship was a 'co-sysop" of the Illuminati bulletin board, which means that he had the ability to review anything on the Illuminati bulletin board and, importantly, maybe able to delete anything on the system. Blankenship's bulletin board Phoenix had published "hacker" information and had solicited "hacker" information relating to passwords, ostensibly to be analyzed in some type of decryption scheme. By February 26, 1990, Kluepfel determined that the Phoenix bulletin board was no longer accessible as he could not "dial" or "log into" it. He reported this to Agent Foley. While Kluepfel advised Agent Foley that Blankenship was an employee of Steve Jackson Games, Inc., and was a user and co-sysop of Illuminati, Kluepfel never had any information whereby he was suspicious of any criminal activity by any of the Plaintiffs in this cause. Kluepfel was, and is, knowledgeable in the operation of computers, computer bulletin boards, the publishing of materials and document by computers, the communications through computer bulletin boards (both public and private communications), and could have "logged" into the Illuminati bulletin board at any time and reviewed all of the information on the bulletin board except for the private communications referred to by the Plaintiffs as electronic communications or electronic mail, but did not do so. Kluepfel had legitimate concerns, both about the 911 document stolen from Bell South and the possibility of a decryption system which could utilize passwords in rapid fashion and could result in intrusions of computer systems, including those of the Bell System.

In February of 1990, Agent Foley was also knowledgeable about computer bulletin boards and he too could have "logged" into Illuminati, become a user and reviewed all public communications on the bulletin board, but did not do so.

By February 28, 1990, when the search warrant affidavit was executed, Agent Foley had received information from reliable sources (Kluepfel, Williams, Spain, Kibbler, Coutorie, and Niedorf, and possibly others (F3)) there had been an unlawful intrusion on the Bell South computer program, the 911 Bell South document was a sensitive and proprietary document, and that computer hackers were attempting to utilize a decryption procedure whereby unlawful intrusions could be made to computer programs including the Defense Department, and these hackers were soliciting passwords so that the decryption procedure could become operational. In addition, Agent Foley was advised Loyd Blankenship had operated his Phoenix bulletin board

from his home, had published the 911 Bell South document in edited form, and had published and communicated that a decryption strategy was available and other "hackers" should submit selective passwords to finalize the decryption scheme for intrusions into computer systems by using a rapid deployment of passwords. Agent Foley was also advised that Blankenship was an employee of Steve Jackson Games and had access to the Illuminati bulletin board as a user and a co-sysop and he may well (and in fact did) have the ability to delete any documents or information in the Steve Jackson Games computers and Illuminati bulletin board. The only information Agent Foley had regarding Steve Jackson Games, Inc. and Steve Jackson was that he thought this was a company that put out games, but he also reviewed a printout of Illuminati on February 25, 1990, which read, "Greetings, Mortal! You have entered the secret computer system of the Illuminati, the on-line home of the world's oldest and largest secret conspiracy. 5124474449300/1200/2400BAUD fronted by Steve Jackson Games, Incorporated. Fnord." The evidence in this case strongly suggests Agent Foley, without any further investigation, misconstrued this information to believe the Illuminati bulletin board was similar in purpose to Blankenship's Phoenix bulletin board, which provided information to and was used by "hackers." Agent Foley believed, in good faith, at the time of the execution of his affidavit on February 28, 1990, there was probable cause to believe Blankenship had the 911 Bell South document and information relating to the decryption scheme stored in his computer at home or perhaps in computers, disks, or in the Illuminati bulletin board at his place of employment at Steve Jackson Games, Inc.; that these materials were involved in criminal activities; and that Blankenship had the ability to delete any information stored on any of these computers and/or disks.

Unfortunately, although he was an attorney and expressly represented this fact in his affidavit, Agent Foley was not aware of the Privacy Protection Act, 42 U.S.C. 2000aa _et seq._, and he conducted no investigation about Steve Jackson Games, Incorporated, although a reasonable investigation of only several hours would have revealed Steve Jackson Games, Inc. was, in fact, a legitimate publisher of information to the public and Mr. Jackson would have cooperated in the investigation. Agent Foley did not know the individual Plaintiffs but did know they were users of Illuminati as he had a list of all users prior to February 28, 1990. Agent Foley did know and understand the Illuminati bulletin board would have users and probably would have stored private electronic communications between users. Notwithstanding the failure of any investigation regarding Steve Jackson Games, Agent Foley and Assistant U. S. Attorney Cook intended to seize and review all of the information and documents in any computer accessible to Blankenship, regardless of what other incidental information would be seized. These intentions were expressly stated in their application for a search warrant and the warrant itself. (F4)

Foley's affidavit, executed on February 28, 1990, was sufficient under the

law for the issuance of a search warrant by the United States Magistrate Judge. The Court does not find from a preponderance of the evidence that the admitted errors in Foley's affidavit were intentional and so material to make the affidavit and issuance of the warrant legally improper. _See, Franks v. Delaware_, 438 U.S. 154, 98 S.Ct. 2674 (1978). The factual errors in the affidavit include the Bell 911 document was a computer program; the Bell 911 document was engineered at a cost of $79,449; the Bell 911 document had been "slightly" edited; articles in _Phrack_ were described as "hacker tutorials;" the Bell 911 document published in Phrack contained a proprietary notice; Blankenship was a computer programmer for Steve Jackson Games, Inc.; Blankenship's alias "Mentor" was listed as an Illuminati bulletin board user; Coutorie, prior to February 28, 1990, provided Foley with information on Steve Jackson Games, Inc.; and that Kluepfel had "logged" into Illuminati. The affidavit and warrant preparation was simply sloppy and not carefully done. Therefore, the Court denies the Plaintiff's contentions relating to the alleged improprieties involved in the issuance of the search warrant.

On March 1, 1990, Agents Foley and Golden executed the search warrant. At the time of the execution, each agent had available computer experts who had been flown to Austin to advise and review the stored information in the computers, the bulletin boards, and disks seized. These computer experts certainly had the ability to review the stored information and, importantly, to copy all information contained in the computers and disks within hours.

During the search of Steve Jackson Games and the seizure of the three computers, over 300 computer disks, and other materials, Agent Golden was orally advised by a Steve Jackson Games, Inc. Employee that Steve Jackson Games, Inc. was in the publishing business. Unfortunately, Agent Golden, like Foley, was unaware of the Privacy Protection Act and apparently attached no significance to this information. The evidence is undisputed that Assistant U. S. Attorney Cook would have stopped the search at the time of this notification had he been contacted.

By March 2, 1990, Agent Foley knew Steve Jackson Games, Inc. was in the publishing business and the seizure included documents intended for publication to the public, including a book and other forms of information. He also knew or had the ability to learn the seizure of the Illuminati bulletin board included private and public electronic communications and E-mail. By March 2, 1990, Agent Foley knew that Steve Jackson Games, Incorporated, and its attorneys in Dallas and Austin, were requesting the immediate return of the properties and information seized, that transcripts of publications and the back-up materials had been seized, and that the seizure of the documents, including business records of Steve Jackson Games, Inc., and their back-up was certain to economically damage Steve Jackson Games, Inc. While Agent Foley had a legitimate concern there might be some type of program designed to delete

the materials, documents, or stored information he was seeking, he admits there was no valid reason why all information seized could not have been duplicated and returned to Steve Jackson Games _within a period of hours and no more than eight days_ from the seizure. In fact, it was months (late June 1990) before the majority of the seized materials was returned. Agent Foley simply was unaware of the law and erroneously believed he had substantial criminal information which obviously was not present, as to date, no arrests or criminal charges have ever been filed against anyone, including Blankenship.

In addition, Agent Foley must have known his seizure of computers, printers, disks and other materials and his refusal to provide copies represented a risk of substantial harm to Steve Jackson Games, Inc. -- under circumstances where he had no reason to believe the corporation or its owner was involved in criminal activity.

The Secret Service denies that its personnel or its delegates read the private electronic communications stored in the seized materials and specifically allege that this information was reviewed by use of key search words only. Additionally, the Secret Service denies the deletion of any information seized with two exceptions of sensitive" or "illegal" information, the deletion of which was consented to by Steve Jackson. However, the preponderance of the evidence, including common sense (F5), establishes that the Secret Service personnel or its delegates did read all electronic communications seized and did delete certain information and communications in addition to the two documents admitted deleted. The deletions by the Secret Service, other than the two documents consented to by Steve Jackson, were done without consent and cannot be justified.

By March 2, 1990, Agent Foley, Agent Golden, and the Secret Service, if aware of the Privacy Protection Act, would have known that they had, by a search warrant, seized work products of materials from a person or entity reasonably believed to have a purpose to disseminate to the public a "book" or "similar form of public communication."

The failure of the Secret Service after March 1, 1990, to -- promptly -- return the seized products of Steve Jackson Games, Incorporated cannot be justified and unquestionably caused economic damage to the corporation.

By March 1, 1990, Steve Jackson Games, Incorporated was apparently recovering from acute financial problems and suffering severe cash flow problems. The seizure of the work product and delays of publication, whether by three weeks or several months, directly impacted on Steve Jackson Games, Incorporated. Eight employees were terminated because they could not be paid as revenues from sales came in much later than expected. However, it is also clear from a preponderance of the evidence that after the calendar year 1990, the publicity surrounding this seizure and the nature of the products sold by Steve Jackson Games, Incorporated had the

effect of increasing, not decreasing, sales. In fact, Steve Jackson Games, Incorporated developed a specific game for sale based upon the March 1, 1990, seizure. The Court declines to find from a preponderance of the evidence there was any economic damage to Steve Jackson Games, Incorporated after the calendar year 1990 as a result of the seizure of March 1, 1990. (F6)

As a result of the seizure of March 1, 1990, and the retention of the equipment and documents seized, Steve Jackson Games, Incorporated sustained out-of-pocket expenses of $8,781.00. The personnel at this corporation had to regroup, rewrite, and duplicate substantial prior efforts to publish the book _Gurps Cyberpunk_ and other documents stored in the computers and the Illuminati bulletin board, explain to their clientele and users of the bulletin board the difficulties of their continuing business to maintain their clientele, to purchase or lease substitute equipment and supplies, to re-establish the bulletin board, and to get the business of Steve Jackson Games, Inc. back in order. The Court has reviewed the evidence regarding annual sales and net income of Steve Jackson Games, Incorporated for 1990 and the years before and after and finds from a preponderance of the evidence there was a 6 percent loss of sales in 1990 due to the seizure and related problems. The evidence was undisputed that there was a 42 percent profit on sales of publications of Steve Jackson Games, Incorporated. Thus, Steve Jackson Games, Incorporated sustained damages in loss of sales in 1990 of $100,617.00 for a loss of profit of $42,259.00 as a direct and proximate result of the seizure of March 1, 1990, and the retention of the documents seized. After 1990, the net sales of Steve Jackson Games, Incorporated continued to increase annually in a traditional proportion as the sales had been increasing from 1988. Thus, from a preponderance of the evidence, the loss of $42,259.00 is consistent with the net income figures of Steve Jackson Games, Incorporated in the years immediately following and preceding 1990.

Regarding damages to Steve Jackson, personally, his own testimony is that by 1990 he was becoming more active in the management of Steve Jackson Games, Incorporated, and spending less time in creative pursuits such as writing. Steve Jackson Games, Incorporated was in such financial condition that Chapter 11 proceedings in bankruptcy were contemplated. Thereafter, the testimony clearly established that Steve Jackson Games reasserted himself in management and was spending substantial time managing the corporation. The Court declines to find from a preponderance of the evidence that Steve Jackson personally sustained any compensatory damages as a result of the conduct of the United States Secret Service.

Elizabeth McCoy, Walter Milliken and Steffan O'Sullivan also allege compensatory damages. These Plaintiffs all had stored electronic communications, or E-mail, on the Illuminati bulletin board at the time of seizure. All three of these Plaintiffs testified that they had public and private communications in storage at the time of the seizure. Steve

Jackson, Elizabeth McCoy, Walter Milliken and Steffan O'Sullivan all testified that following June of 1990 some of their stored electronic communications, or E-mail, had been deleted. It is clear, as hereinafter set out, that the conduct of the United States Secret Service violated two of the three statutes which the causes of action of the Plaintiffs are based and, therefore, there are statutory damages involved, but the Court declines to find from a preponderance of the evidence that any of the individual Plaintiffs sustained any compensatory damages.

II.
a.

PRIVACY PROTECTION ACT

(First Amendment Privacy Protection)

42 U.S.C. 2000aa et seq.

The United States Secret Service, by Agent Foley and Assistant United States Attorney Cox, sought and obtained an order from a United States Magistrate Judge to _search_ for and _seize_ and thereafter _read_ the information stored and contained in "computer hardware (including, but not limited to, central processing unit(s) monitors, memory devices, modem(s), programming equipment, communication equipment, disks, and printers) and computer software (including, but not limited to) memory disks, floppy disks, storage media) and written material and documents relating to the use of the computer system (including network access files), documentation relating to the attacking of computers and advertising the results of computer attacks (including telephone numbers and location information), and financial documents and licensing documentation relative to the compute programs and equipment at the business known as Steve Jackson Games which constitute evidence, instrumentalities, and fruits of federal crimes, including interstate transportation of stolen property (18 U.S.C. 2314) and interstate transportation of computer access information (18 U.S.C. 1030(a)(6)).' See, Warrant Application and Order.

On March 1, 1990, the Secret Service seized the following property on the premises of Steve Jackson Games, Inc.: Compuadd keyboard; Packard-Bell monitor; DKT computer; cardboard box containing disks, miscellaneous papers and circuit boards; Splat Master gun with "Mentor" on barrel; Hewlett-Packard laser jet printer; BTC keyboard with cover; IBM personal computer 5150 (disassembled); Seagate Tech hard disk; 2400 modem 1649-1795 with power supply and disk; IBM keyboard; Amdek mode 310A; bulletin board back-up files (approximately 150); Empac International Corporation XT computer; "WWIV" users manual; red box of floppy disks; miscellaneous papers and notes from desk; floppy disk entitled "Phoenix setup." _See_, Warrant Return.

The evidence establishes the actual information seized, including both the primary source and back-up materials of the draft of _Gurps Cyberpunk_, a book intended for immediate publication (within days to weeks), drafts of magazine and magazine articles to be published, business records of Steve Jackson Games, Incorporated (including contracts and drafts of articles by writers of Steve Jackson Games, Incorporated), the Illuminati bulletin board and its contents (including public announcements, published newsletter articles submitted to the public for review, public comment on the articles submitted and electronic mail containing both private and public communications). Notwithstanding over 300 floppy disks being seized, the evidence introduced during trial was not clear as to what additional information was seized during the search warrant execution. However, the evidence is clear that on March 1, 1990, "work product materials," as defined in 42 U.S.C. 2000aa-7(b), was obtained as well as materials constituting "documentary materials" as defined in the same provision. (F7)

The Privacy Protection Act, 42 U.S.C. 2000aa, dictates: "Notwithstanding any other law, it shall be unlawful for a government officer or employee, in connection with the investigation . . . of a criminal offense to search for or seize any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, broadcast, or other similar form of public communication . . . ." _See_, 42 U.S.C. Sec. 2000aa(a).

Assuming Agent Foley was knowledgeable of the Privacy Protection Act (which he was not), neither he nor Assistant United States Attorney Cox had any information which would lead them to believe that Steve Jackson Games, Incorporated published books and materials and had a purpose to disseminate to the public its publications. Their testimony is simply they thought it a producer of games. As heretofore stated, the Court feels Agent Foley failed to make a reasonable investigation of Steve Jackson Games, Incorporated when it was apparent his intention was to take substantial properties belonging to the corporation, the removal of which could have a substantial effect on the continuation of business. Agent Foley, it appears, in his zeal to obtain evidence for the criminal investigation, simply concluded Steve Jackson Games, Incorporated was somehow involved in Blankenship's alleged activities because of the wording of the Illuminati bulletin board menu. In any event, the Court declines to find from a preponderance of the evidence that on March 1, 1990, Agent Foley or any other employee or agent of the United States had reason to believe that property seized would be the work product materials of a person believed to have a purpose to disseminate to the public a newspaper, book, broadcast or other similar form of public communication. (F8)

During the search on March 1, and on March 2, 1990, the Secret Service was specifically advised of facts that put its employees on notice of probable violations of the Privacy Protection Act. It is no excuse that Agents

Foley and Golden were not knowledgeable of the law. On March 2, 1990, and thereafter, the conduct of the United States Secret Service was in violation of 42 U.S.C. 2000aa _et seq_. It is clear the Secret Service continued the seizure of property of Steve Jackson Games, Incorporated including information and documents through late June of 1990. Immediate arrangements could and should have been made on March 2, 1990, whereby copies of all information seized could have been made. The government could and should have requested Steve Jackson as chief operating officer of the corporation to cooperate and provide the information available under the law. The Secret Service's refusal to return information and property requested by Mr. Jackson and his lawyers in Dallas and Austin constituted a violation of the statute. Regarding any information seized that would constitute "documentary materials" (whereby the defensive theory of 42 U.S.C. 2000aa(b)(3) might apply) there would have been no problem as the property was in the possession of the United States Secret Service and their experts and Steve Jackson were present to ensure no destruction, alteration or concealment of information contained therein. In any event, it is the seizure of the "work product materials" that leads to the liability of the United States Secret Service and the United States in this case. Pursuant to 42 U.S.C. 2000aa-6, the Court finds from a preponderance of the evidence that Steve Jackson Games, Incorporated is entitled to judgment against the United States Secret Service and the United States of America for its expenses of $8,781.00 and its economic damages of $42,259.00. The Court declines to find from a preponderance of the evidence other damages of Steve Jackson Games, Incorporated or liability of the United States Secret Service or the United States of America to any other Plaintiff under the provisions of the Privacy Protection Act.

b.

WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION
AND INTERCEPTION OF ORAL COMMUNICATIONS
18 U.S.C. 2510 et seq.

The Plaintiffs allege the United States Secret Service's conduct also violated 18 U.S.C. 2510, et seq., as it constituted intentional interceptions of "electronic communication." They allege the interception occurred at the time of seizure or, perhaps, at the time of review of the communication subsequent to the seizure. There is no question the individual Plaintiffs had private communications stored in Illuminati at the time of the seizure and the court has found from a preponderance of the evidence the Secret Service intended not only to seize and read these communications, but, in fact, did read the communications and thereafter deleted or destroyed some communications either intentionally or accidentally. The Defendants contend there is no violation of this particular statute under the facts of this case because there never was any unlawful "interception" within the meaning of the statute.

Alternatively, the Defendants contend that the "good faith reliance" on the search warrant issued by the United States Magistrate Judge is a complete defense under Section 2520.

The Government relies on the 1976 Fifth Circuit case of the _United States v. Turk_, 526 F.2d 654 (5th Cir. 1976), _cert denied_, 429 U.S. 823, 97 S.Ct. 74 (1976), and its interpretation of the statutory definition of "interception." In _Turk_, police officers listened to the contents of a cassette tape without first obtaining a warrant. The court concluded this was not an "interception" under 18 U.S.C. Sec. 2510 et seq.

>>Whether the seizure and replaying of the cassette tape by the officers was also an "interception" depends on the definition to be given "aural acquisition.' Under one conceivable reading, and 'aural acquisition" could be said to occur whenever someone physically hears the contents of a communication, and thus the use of the tape player by the officers to hear the previously recorded conversation might fall within the definition set out above. No explicit limitation of coverage to contemporaneous "acquisitions" appears in the Act.

>>We believe that a different interpretation -- one which would exclude from the definition of "intercept" the replaying of a previously recorded conversation -- has a much firmer basis in the language of Sec. 2510(4) and in logic, and corresponds more closely to the policies reflected in the legislative history. The words acquisition... through the use of any ... device" suggest that the central concern is with the activity engaged in a the time of the oral communication which causes such communication to be overheard by uninvited listeners. If a person secrets a recorder in a room and thereby records a conversation between two others, an "acquisition" occurs at the time the recording is made. This acquisition itself might be said to be "aural" because the contents of the conversation are preserved in 2 form which permits the later aural disclosure of the contents. Alternatively, a court facing the issue might conclude that an "aural acquisition" is accomplished only when two steps are completed -- the initial acquisition by the device and the hearing of the communication by the person or persons responsible for the recording. Either of these definitions would require participation by the one charged with an "interception" in the contemporaneous acquisition of the communication through the use to the device. The argument that a new and different aural acquisition" occurs each time a recording of an oral communication is replayed is unpersuasive. That would mean that innumerable "interceptions," and thus violations of the Act, could follow from a single recording .

_Id._, at 657-658 (footnotes omitted). While the Fifth Circuit authority relates to the predecessor statute, Congress intended no change in the existing definition of 'intercept" in amending the statute in 1986. _See_,

S. Rep. No. 541, 99th Cong., 2nd Sess. 13 (1986), _reprinted in_ 1986 U.S.C.C.A.N. 3555, 3567 ("Section 101(a)(3) of the ELECTRONIC COMMUNICATIONS PRIVACY ACT amends the definition of the term "intercept" in current section 2510(4) of electronic communications. The definition of "intercept" under current law is retained with respect to wire and oral communications except that the term "or other" is inserted after "aural." This amendment clarifies that it is illegal to intercept the non-voice portion of a wire communication."). The Court finds this argument persuasive when considering the Congressional enactment of the Stored Wire and Electronic Communications and Transactional Records Access Act, 18 U.S.C. 2701, _et seq_.

The Court declines to find liability for any Plaintiff against the Defendants pursuant to the Wire and Electronic Communications Interception and Interception of Oral Communications Act, 18 U.S.C. 2510, et seq., and specifically holds that the alleged "interceptions" under the facts of this case are not 'interceptions contemplated by the Wire and Electronic Communications Interception and Interception of Oral Communications Act. It simply has no applicability to the facts of this case.

c.

STORED WIRE AND ELECTRONIC COMMUNICATIONS
AND TRANSACTIONAL RECORDS ACCESS
18 U.S.C. Sec. 2701 et seq.

Prior to February 28, 1990, Agent Foley, Assistant United States Attorney Cox, and the computer consultants working with them were cognizant of public computer bulletin boards and the use of electronic communications and E-mail through them. Each of the persons involved in this investigation, including Agent Foley, had the knowledge and opportunity to log into the Illuminati bulletin board, review its menu and user lists, obtain passwords, and thereafter review all information available to the public. In fact, Agent Foley erroneously thought Kluepfel had done this when a printout of Illuminati documents dated February 25, 1990, was recieved. When Foley applied for the search warrant on February 28, 1990, he knew the Illuminati bulletin board provided services to the public whereby its users could store public and private electronic communications. While Foley admits no knowledge of the Privacy Protection Act and its provisions protecting publishers of information 'o the public, he testified he was knowledgeable regarding the Wire and Electronic Communications Interception and Interception of Oral Communications Act. But, Foley never thought of the law's applicability under the facts of this case. Steve Jackson Games, Inc., through its Illuminati bulletin board services, was a "remote computing service" within the definition of Section 2711, and, therefore, the only procedure available to the Secret Service to obtain _"disclosure"_ of the contents of electronic communications was to comply with this statute. _See_, 18 U.S.C. 2703.

Agent Foley and the Secret Service, however, wanted more than "disclosure' of the contents of the communication. As the search warrant application evidences, the Secret Service wanted _seizure_ of all information and the authority to review and read all electronic communications, both public and private. A court order for such disclosure is only to issue if "there is a reason to believe the contents of a[n] . . . electronic communication . . . are relevant to a legitimate law enforcement inquiry." _See_, 18 U.S.C. Sec. 2703(d). Agent Foley did not advise the United States Magistrate Judge, by affidavit or otherwise, that the Illuminati bulletin board contained private electronic communications between users or how the disclosure of the content of these communications could relate to his investigation. Foley's only knowledge was that Blankenship had published part of the 911 document and decryption information in his Phoenix bulletin board, was employed at Steve Jackson Games, Inc., and could have the ability to store and delete these alleged unlawful documents in the computers or Illuminati bulletin board at Steve Jackson Games, Incorporated. At Agent Foley's specific request, the application and affidavit for the search warrant were sealed. The evidence establishes the Plaintiffs were not able to ascertain the reasons for the March 1, 1990 seizure until after the return of most of the property in June of 1990, and then only by the efforts of the offices of both United States Senators of the State of Texas. The procedures followed by the Secret Service in this case virtually eliminated the safeguards contained in the statute. For example, no Plaintiff was on notice that the search or seizure order was made pursuant to this statute and that Steve Jackson Games, Incorporated could move to quash or modify the order or eliminate or reduce any undue burden on it by reason of the order. _See_, 18 U.S.C. Sec. 2703(d). The provisions of the statute regarding the preparation of back-up copies of the documents or information seized were never utilized or available. _See_, 18 U.S.C. Sec. 2704. Agent Foley stated his concern was to prevent the destruction of the documents' content and for the Secret Service to take the time necessary to carefully review all of the information seized. He feared Blankenship could possibly delete the incriminating documents or could have programmed destruction in some manner. Notwithstanding that any alteration or destruction by Blankenship, Steve Jackson, or anyone else would constitute a criminal offense under this statute, Foley and the Secret Service seized -- not just obtained disclosure of the content -- all of the electronic communications stored in the Illuminati bulletin board involving the Plaintiffs in this case. This conduct exceeded the Government's authority under the statute.

The Government Defendants contend there is no liability for alleged violation of the statute as Foley and the Secret Service had a "good faith" reliance on the February 28, 1990, court order/search warrant. The Court declines to find this defense by a preponderance of the evidence in this case.

Steve Jackson Games, Incorporated, as the provider and each individual

Plaintiffs as either subscribers or customers were "aggrieved" by the conduct of the Secret Service in the violation of this statute. While the Court declines to find from a preponderance of the credible evidence the compensatory damages sought by each Plaintiff, the Court will assess the statutory damages of $1,000.00 for each Plaintiff.

III. SUMMARY

This is a complex case. It is still not clear how sensitive and/or proprietary the 911 document. was (2nd is) or how genuinely harmful the potential decryption scheme may have been or if either were discovered by the Secret Service in the information seized on March 1, 1990. The fact that no criminal charges have ever been filed and the investigation remains "on going" is, of course, not conclusive.

The complexity of this case results from the Secret Service's insufficient investigation and its lack of knowledge of the specific laws that could apply to their conduct on February 28, 1990 and thereafter. It appears obvious neither the government employees nor the Plaintiffs or their lawyers contemplated the statute upon which this case is brought back in February, March, April, May or June of 1990. But this does not provide assistance to the defense of the case. The Secret Service and its personnel are the entities that citizens, like each of the Plaintiffs, rely upon and look to protect their rights and properties. The Secret Service conduct resulted in the seizure of property, products, business records, business documents, and electronic communications of a corporation and four individual citizens that the statutes were intended to protect.

It may well be, as the Government Defendants contend, these statutes relied upon by the Plaintiffs should not apply to the facts of this case, as these holdings may result in the government having great difficulties in obtaining information or computer documents -representing illegal activities. But this Court cannot amend or rewrite the statutes involved. The Secret Service must go to the Congress for relief. Until that time, this Court recommends better education, investigation and strict compliance with the statutes as written.

The Plaintiffs are ordered to submit application for attorney's fees and costs with appropriate supporting affidavits within ten (10) days of the date of this order. The Defendants will have ten days thereafter to file their responses.

SIGNED this the 12 day of March, 1993.

Sam Sparks, United States District Judge

FOOTNOTES

1. While the content of these publications are not similar to those of daily newspapers, news magazines, or other publications usually thought of by this Court as disseminating information to the public, these products come within the literal language of the Privacy Protection Act.

2. A "hacker" is an individual who accesses another's computer system without authority.

3. Kluepfel, Williams, Spain and Kibbler are employees of Bell South; Coutorie is a University of Texas Systems investigator assigned to investigate computer hacking; and Niedorf is a hacker involved in the Illinois bulletin board system.

4. The Court does fault Agent Foley and the Secret Service on the failure to make any investigation of Steve Jackson Games, Inc. prior to March 1, 1990, and to contact Steve Jackson in an attempt to enlist his cooperation and obtain information from him as there was never any basis to suspect Steve Jackson or Steve Jackson Games, Inc. of any criminal activity, and there could be no questions the seizure of computers, disks, and bulletin board and all information thereon, including all back-up materials would have an adverse effect (including completely stopping all activities) on the business of Steve Jackson Games, Inc. and the users of Illuminati bulletin board.

5. The application and the search warrant itself was worded by Foley and Cook so that all information would be "read" by the Secret Service.

6. The Court finds the testimony of Joanne Midwikis, an accountant who testified on behalf of Steve Jackson Games, Inc. and Steve Jackson, on damages suffered by Steve Jackson Games, Inc. and Steve Jackson was not credible.

7. If the Secret Service, in the performance of executing Court order, had only obtained and taken the 911 document or alleged decryption materials, application of the definitions of "documentary materials" and "work product materials" would logically result in no violation of the statute under the circumstances of this case. It was the seizing all documents and information and, thereafter, the failure to promptly return the information seized which leads to violation of the statute.

8. The legislative history to the Privacy Protection Act states:

...the Committee recognized a problem for the law enforcement officer, who seeking to comply with the statute, might be uncertain whether the materials he sought were work product or nonwork product and that they were intended for publication. Therefore, in the interests of allowing for

some objective measure for judgment by the office, the Committee has provided that the work product must be possessed by someone "reasonably believed" to have a purpose to communicate to the public.

S. Rep. No. 874, 96th Cong., 2nd Sess., 10 (1980), _reprinted in_ 1980 U.S.C.C.A.N. 3950, 3957. As the Court has stated, Agent Foley with only a few hours of investigation would have "reasonably believed" Steve Jackson Games, Incorporated had "a purpose to communicate to the public." Therefore, under an objective standard, assuming a reasonable investigation, Agent Foley and the Secret Service violated the statute on March 1, 1990. However, Agent Foley was not aware of the Privacy Protection Act and was therefore not "seeking to comply" with its requirements. Consequently, the Court found on March 1, 1990 neither Agent Foley or any other employee or agent of the United States "reasonably believed" the materials seized were work product or Steve Jackson Games, Incorporated had a "purpose to disseminate to the public."

Fifth Circuit Opinion On Appeal

STEVE JACKSON GAMES, INCORPORATED, et al., Plaintiffs-Appellants,

v.

UNITED STATES SECRET SERVICE, et al., Defendants,

United States Secret Service and United States of America, Defendants-

Appellees.

No. 93-8661.

United States Court of Appeals,

Fifth Circuit.

Oct. 31, 1994.

Peter D. Kennedy, R. James George, Jr., George, Donaldson & Ford, Austin, TX, for appellants.

Sharon Steele, Washington, DC, for amicus curiae Electronic Frontier Foundation.

Scott McIntosh, Barbara Herwig, U.S. Dept. of Justice, Washington, DC, for appellees.

Appeal from the United States District Court for the Western District of Texas.

Before HIGGINBOTHAM, JONES and BARKSDALE, Circuit Judges.

RHESA HAWKINS BARKSDALE, Circuit Judge:

The narrow issue before us is whether the seizure of a computer, used to operate an electronic bulletin board system, and containing private electronic mail which had been sent to (stored on) the bulletin board, but not read (retrieved) by the intended recipients, constitutes an unlawful intercept under the Federal Wiretap Act, 18 U.S.C. s 2510, et seq., as amended by Title I of the Electronic Communications Privacy Act of 1986, Pub.L. No. 99-508, Title I, 100 Stat. 1848 (1986). We hold that it is not, and therefore AFFIRM.

I.

The district court's findings of fact are not in dispute. See Steve Jackson Games, Inc. v. United States Secret Service, 816 F.Supp. 432 (W.D.Tex.1993). Appellant Steve Jackson Games, Incorporated (SJG), publishes books, magazines, role-playing games, and related products. Starting in the mid-1980s, SJG operated an electronic bulletin board system, called "Illuminati" (BBS), from one of its computers. SJG used the BBS to post public information about its business, games, publications, and the role-playing hobby; to facilitate play-testing of games being developed; and to communicate with its customers and free-lance writers by electronic mail (E- mail).

Central to the issue before us, the BBS also offered customers the ability to send and receive private E-mail. Private E-mail was stored on the BBS computer's hard disk drive temporarily, until the addressees "called" the BBS (using their computers and modems) and read their mail. After reading their E- mail, the recipients could choose to either store it on the BBS computer's hard drive or delete it. In February 1990, there were 365 BBS users. Among other uses, appellants Steve Jackson, Elizabeth McCoy, William Milliken, and Steffan O'Sullivan used the BBS for communication by private E-mail.

In October 1988, Henry Kluepfel, Director of Network Security Technology (an affiliate Bell Company), began investigating the unauthorized duplication and distribution of a computerized text file, containing information about Bell's emergency call system. In July 1989, Kluepfel informed Secret Service Agent Foley and an Assistant United States Attorney in Chicago about the unauthorized distribution. In early February 1990, Kluepfel learned that the document was available on the "Phoenix Project" computer bulletin board, which was operated by Loyd Blankenship in Austin, Texas; that Blankenship was an SJG employee; and that, as a co-systems operator of the BBS, Blankenship had the ability to review and, perhaps, delete any data on the BBS.

On February 28, 1990, Agent Foley applied for a warrant to search SJG's premises and Blankenship's residence for evidence of violations of 18 U.S.C. ss 1030 (proscribes interstate transportation of computer access information) and 2314 (proscribes interstate transportation of stolen property). A search warrant for SJG was issued that same day, authorizing the seizure of, inter

alia,

> [c]omputer hardware ... and computer software ... and ... documents relating to the use of the computer system ..., and financial documents and licensing documentation relative to the computer programs and equipment at ... [SJG] ... which constitute evidence ... of federal crimes.... This warrant is for the seizure of the above described computer and computer data and for the authorization to read information stored and contained on the above described computer and computer data.

The next day, March 1, the warrant was executed by the Secret Service, including Agents Foley and Golden. Among the items seized was the computer which operated the BBS. At the time of the seizure, 162 items of unread, private E-mail were stored on the BBS, including items addressed to the individual appellants. Despite the Secret Service's denial, the district court found that Secret Service personnel or delegates read and deleted the private E-mail stored on the BBS.

Appellants filed suit in May 1991 against, among others, the Secret Service and the United States, claiming, inter alia, violations of the Privacy Protection Act, 42 U.S.C. s 2000aa, et seq. [FN1]; the Federal Wiretap Act, as amended by Title I of the Electronic Communications Privacy Act (ECPA), 18 U.S.C. ss 2510-2521 (proscribes, inter alia, the intentional interception of electronic communications); and Title II of the ECPA, 18 U.S.C. ss 2701-2711 (proscribes, inter alia, intentional access, without authorization, to stored electronic communications). [FN2]

The district court held that the Secret Service violated the Privacy Protection Act, and awarded actual damages of $51,040 to SJG; and that it violated Title II of the ECPA by seizing stored electronic communications without complying with the statutory provisions, and awarded the statutory damages of $1,000 to each of the individual appellants. And, it awarded appellants $195,000 in attorneys' fees and approximately $57,000 in costs. But, it held that the Secret Service did not "intercept" the E-mail in violation of Title I of the ECPA, 18 U.S.C. s 2511(1)(a), because its acquisition of the contents of the electronic communications was not contemporaneous with the transmission of those communications.

II.

As stated, the sole issue is a very narrow one: whether the seizure of a computer on which is stored private E-mail that has been sent to an electronic bulletin board, but not yet read (retrieved) by the recipients, constitutes an "intercept" proscribed by 18 U.S.C. s 2511(1)(a). [FN3] Section 2511 was enacted in 1968 as part of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, often referred to as the Federal Wiretap Act. Prior to the 1986 amendment by Title I of the ECPA, it covered only wire and oral communications. Title I of the ECPA extended that coverage to electronic communications. [FN4] In relevant part, s 2511(1)(a) proscribes "intentionally intercept[ing] ... any wire, oral, or electronic communication", unless the intercept is authorized by court order or by other exceptions not relevant here. Section 2520 authorizes, inter alia, persons whose electronic communications are intercepted in violation of s 2511 to bring a civil action against the interceptor for actual damages, or for statutory damages of $10,000 per violation or $100 per day of the violation, whichever is greater. 18 U.S.C. s 2520. [FN5]

The Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. s 2510(4). The district court, relying on our court's interpretation of intercept in United States v. Turk, 526 F.2d 654 (5th Cir.), cert. denied, 429 U.S. 823, 97 S.Ct. 74, 50 L.Ed.2d 84 (1976), held that the Secret Service did not intercept the communications, because its acquisition of the contents of those communications was not contemporaneous with their transmission. In Turk, the government seized from a suspect's vehicle an audio tape of a prior conversation between the suspect and Turk. (Restated, when the conversation took place, it was not recorded contemporaneously by the government.) Our court held that replaying the previously recorded conversation was not an "intercept", because an intercept "require[s] participation by the one charged with an 'interception' in the contemporaneous acquisition of the communication through the use of the device". Id. at 658.

Appellants agree with Turk's holding, but contend that it is not applicable, because it "says nothing about government action that both acquires the communication prior to its delivery, and

prevents that delivery." (Emphasis by appellants.) Along that line, appellants note correctly that Turk's interpretation of "intercept" predates the ECPA, and assert, in essence, that the information stored on the BBS could still be "intercepted" under the Act, even though it was not in transit. They maintain that to hold otherwise does violence to Congress' purpose in enacting the ECPA, to include providing protection for E-mail and bulletin boards. For the most part, appellants fail to even discuss the pertinent provisions of the Act, much less address their application. Instead, they point simply to Congress' intent in enacting the ECPA and appeal to logic (i.e., to seize something before it is received is to intercept it).

But, obviously, the language of the Act controls. In that regard, appellees counter that "Title II, not Title I, ... governs the seizure of stored electronic communications such as unread e-mail messages", and note that appellants have recovered damages under Title II. Understanding the Act requires understanding and applying its many technical terms as defined by the Act, as well as engaging in painstaking, methodical analysis. As appellees note, the issue is not whether E-mail can be "intercepted"; it can. Instead, at issue is what constitutes an "intercept".

Prior to the 1986 amendment by the ECPA, the Wiretap Act defined "intercept" as the "aural acquisition" of the contents of wire or oral communications through the use of a device. 18 U.S.C. s 2510(4) (1968). The ECPA amended this definition to include the "aural or other acquisition of the contents of ... wire, electronic, or oral communications...." 18 U.S.C. s 2510(4) (1986) (emphasis added for new terms). The significance of the addition of the words "or other" in the 1986 amendment to the definition of "intercept" becomes clear when the definitions of "aural" and "electronic communication" are examined; electronic communications (which include the non- voice portions of wire communications), as defined by the Act, cannot be acquired aurally.

Webster's Third New International Dictionary (1986) defines "aural" as "of or relating to the ear" or "of or relating to the sense of hearing". Id. at 144. And, the Act defines "aural transfer" as "a transfer containing the human voice at any point between and including the point of origin and the point of reception." 18 U.S.C. s 2510(18). This definition is extremely important for purposes of understanding the definition of a "wire communication", which is defined by the Act as

> any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) ... and such term includes any electronic storage of such communication.

18 U.S.C. s 2510(1) (emphasis added). In contrast, as noted, an "electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system ... but does not include ... any wire or oral communication...." 18 U.S.C. s 2510(12) (emphasis added).

Critical to the issue before us is the fact that, unlike the definition of "wire communication", the definition of "electronic communication" does not include electronic storage of such communications. See 18 U.S.C. s 2510(12). See note 4, supra. [FN6] "Electronic storage" is defined as

> (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
> (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication....

18 U.S.C. s 2510(17) (emphasis added). The E-mail in issue was in "electronic storage". Congress' use of the word "transfer" in the definition of "electronic communication", and its omission in that definition of the phrase "any electronic storage of such communication" (part of the definition of "wire communication") reflects that Congress did not intend for "intercept" to apply to "electronic communications" when those communications are in "electronic storage". [FN7]

We could stop here, because "[i]ndisputably, the goal of statutory construction is to ascertain legislative intent through the plain language of a statute--without looking to legislative history or other extraneous sources". Stone v. Caplan (Matter of Stone), 10 F.3d 285, 289 (5th Cir.1994). But, when interpreting a

statute as complex as the Wiretap Act, which is famous (if not infamous) for its lack of clarity, see, e.g., Forsyth v. Barr, 19 F.3d 1527, 1542-43 (5th Cir.), cert. denied, --- U.S. ----, --- S.Ct. ----, --- L.Ed.2d ---- (1994), we consider it appropriate to note the legislative history for confirmation of our understanding of Congress' intent. See id. at 1544.

As the district court noted, the ECPA's legislative history makes it crystal clear that Congress did not intend to change the definition of "intercept" as it existed at the time of the amendment. See 816 F.Supp. at 442 (citing S.Rep. No. 99-541, 99th Cong., 2d Sess. 13 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3567). The Senate Report explains: Section 101(a)(3) of the [ECPA] amends the definition of the term "intercept" in current section 2510(4) of title 18 to cover electronic communications. The definition of "intercept" under current law is retained with respect to wire and oral communications except that the term "or other" is inserted after "aural." This amendment clarifies that it is illegal to intercept the nonvoice portion of a wire communication. For example, it is illegal to intercept the data or digitized portion of a voice communication. 1986 U.S.C.C.A.N. at 3567.

Our conclusion is reinforced further by consideration of the fact that Title II of the ECPA clearly applies to the conduct of the Secret Service in this case. Needless to say, when construing a statute, we do not confine our interpretation to the one portion at issue but, instead, consider the statute as a whole. See, e.g., United States v. McCord, --- F.3d ----, ----, 1994 WL 523211, at *6 (5th Cir.1994) (citing N. Singer, 2A Sutherland Statutory Construction, s 46.05, at 103 (5th ed. 1992)). Title II generally proscribes unauthorized access to stored wire or electronic communications. Section 2701(a) provides:

> Except as provided in subsection (c) of this section whoever--
>
> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
>
> (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents

> authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished....

18 U.S.C. s 2701(a) (emphasis added).

As stated, the district court found that the Secret Service violated s 2701 when it intentionally accesse[d] without authorization a facility [the computer] through which an electronic communication service [the BBS] is provided ... and thereby obtain[ed] [and] prevent[ed] authorized access [by appellants] to a[n] ... electronic communication while it is in electronic storage in such system. 18 U.S.C. s 2701(a). The Secret Service does not challenge this ruling.

We find no indication in either the Act or its legislative history that Congress intended for conduct that is clearly prohibited by Title II to furnish the basis for a civil remedy under Title I as well. Indeed, there are persuasive indications that it had no such intention.

First, the substantive and procedural requirements for authorization to intercept electronic communications are quite different from those for accessing stored electronic communications. For example, a governmental entity may gain access to the contents of electronic communications that have been in electronic storage for less than 180 days by obtaining a warrant. See 18 U.S.C. s 2703(a). But there are more stringent, complicated requirements for the interception of electronic communications; a court order is required. See 18 U.S.C. s 2518.

Second, other requirements applicable to the interception of electronic communications, such as those governing minimization, duration, and the types of crimes that may be investigated, are not imposed when the communications at issue are not in the process of being transmitted at the moment of seizure, but instead are in electronic storage. For example, a court order authorizing interception of electronic communications is required to include a directive that the order shall be executed "in such a way as to minimize the interception of communications not otherwise subject to interception". 18 U.S.C. s 2518(5). Title II of the ECPA does not contain this requirement for warrants authorizing access to stored electronic communications. The purpose of the minimization

requirement is to implement "the constitutional obligation of avoiding, to the greatest possible extent, seizure of conversations which have no relationship to the crimes being investigated or the purpose for which electronic surveillance has been authorized". James G. Carr, The Law of Electronic Surveillance, s 5.7(a) at 5-28 (1994).

Obviously, when intercepting electronic communications, law enforcement officers cannot know in advance which, if any, of the intercepted communications will be relevant to the crime under investigation, and often will have to obtain access to the contents of the communications in order to make such a determination. Interception thus poses a significant risk that officers will obtain access to communications which have no relevance to the investigation they are conducting. That risk is present to a lesser degree, and can be controlled more easily, in the context of stored electronic communications, because, as the Secret Service advised the district court, technology exists by which relevant communications can be located without the necessity of reviewing the entire contents of all of the stored communications. For example, the Secret Service claimed (although the district court found otherwise) that it reviewed the private E-mail on the BBS by use of key word searches.

Next, as noted, court orders authorizing an intercept of electronic communications are subject to strict requirements as to duration. An intercept may not be authorized "for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days". 18 U.S.C. s 2518(5). There is no such requirement for access to stored communications.

Finally, as also noted, the limitations as to the types of crimes that may be investigated through an intercept, see 18 U.S.C. s 2516, have no counterpart in Title II of the ECPA. See, e.g., 18 U.S.C. s 2703(d) (court may order a provider of electronic communication service or remote computing service to disclose to a governmental entity the contents of a stored electronic communication on a showing that the information sought is "relevant to a legitimate law enforcement inquiry").

In light of the substantial differences between the statutory procedures and requirements for obtaining authorization to

intercept electronic communications, on the one hand, and to gain access to the contents of stored electronic communications, on the other, it is most unlikely that Congress intended to require law enforcement officers to satisfy the more stringent requirements for an intercept in order to gain access to the contents of stored electronic communications. [FN8]

At oral argument, appellants contended (for the first time) that Title II's reference in s 2701(c) to s 2518 (which sets forth the procedures for the authorized interception of wire, oral, or electronic communications) reflects that Congress intended considerable overlap between Titles I and II of the ECPA. [FN9] As stated, s 2701(a) prohibits unauthorized access to stored wire or electronic communications. Subsection (c) of s 2701 sets forth the exceptions to liability under subsection (a), which include conduct authorized:

> (1) by the person or entity providing a wire or electronic communications service;
>
> (2) by a user of that service with respect to a communication of or intended for that user; or
>
> (3) in section 2703, 2704 or 2518 of this title.

18 U.S.C. s 2701(c) (emphasis added). [FN10]

Appellants overemphasize the significance of this reference to s 2518. As discussed in notes 6-7, supra, it is clear that Congress intended to treat wire communications differently from electronic communications. Access to stored electronic communications may be obtained pursuant to a search warrant, 18 U.S.C. s 2703; but, access to stored wire communications requires a court order pursuant to s 2518. Because s 2701 covers both stored wire and electronic communications, it was necessary in subsection (c) to refer to the different provisions authorizing access to each.

III.

For the foregoing reasons, the judgment is AFFIRMED.

FN1. Section 2000aa(a) provides that it is unlawful for a

government officer or employee, in connection with the investigation ... of a criminal offense, to search for or seize any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication.... Among the items seized was a draft of GURPS Cyberpunk, a book intended by SJG for immediate publication. It was one of a series of fantasy role-playing game books SJG published. "GURPS" is an acronym for SJG's "Generic Universal Roleplaying System". "Cyberpunk" refers to a science fiction literary genre which became popular in the 1980s, which is characterized by the fictional interaction of humans with technology and the fictional struggle for power between individuals, corporations, and government.

FN2. Kluepfel, the Assistant United States Attorney, and Agents Foley and Golden were also sued. In addition to the statutory claims, appellants also claimed violations of the First and Fourth Amendments to the United States Constitution. And, in September 1992, they added state law claims for conversion and invasion of privacy. Prior to trial, the claims against the individuals were dismissed, and appellants withdrew their constitutional and state law claims.

FN3. Appellants raised two other issues regarding damages, but later advised that they have been settled. And, prior to briefing, the Secret Service dismissed its cross-appeal.

FN4. An "electronic communication" is defined as: any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include-- (A) the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit; (B) any wire or oral communication; (C) any communication made through a tone-only paging device; or (D) any communication from a tracking device (as defined in section 3117 of this title).... 18 U.S.C. s 2510(12).

FN5. Title I of the ECPA increased the statutory damages for unlawful interception from $1,000 to $10,000. See Bess v. Bess, 929 F.2d 1332, 1334 (8th Cir.1991). On the other hand, as noted, Title II authorizes an award of "the actual damages suffered by the

plaintiff and any profits made by the violator as a result of the violation, but in no case ... less than the sum of $1000". 18 U.S.C. s 2707(c). As discussed, the individual appellants each received Title II statutory damages of $1,000.

FN6. Wire and electronic communications are subject to different treatment under the Wiretap Act. The Act's exclusionary rule, 18 U.S.C. s 2515, applies to the interception of wire communications, including such communications in electronic storage, see 18 U.S.C. s 2510(1), but not to the interception of electronic communications. See 18 U.S.C. s 2518(10)(a); United States v. Meriwether, 917 F.2d 955, 960 (6th Cir.1990); S.Rep. No. 99-541, 99th Cong., 2d Sess. 23 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3577. And, the types of crimes that may be investigated by means of surveillance directed at electronic communications, 18 U.S.C. s 2516(3) ("any federal felony"), are not as limited as those that may be investigated by means of surveillance directed at wire or oral communications. See 18 U.S.C. s 2516(1) (specifically listed felonies).

FN7. Stored wire communications are subject to different treatment than stored electronic communications. Generally, a search warrant, rather than a court order, is required to obtain access to the contents of a stored electronic communication. See 18 U.S.C. s 2703(a). But, compliance with the more stringent requirements of s 2518, including obtaining a court order, is necessary to obtain access to a stored wire communication, because s 2703 expressly applies only to stored electronic communications, not to stored wire communications. See James G. Carr, The Law of Electronic Surveillance, s 4.10, at 4-126--4-127 (1994) (citing H.R.Rep. No. 99-647, 99th Cong., 2d Sess. 67-68 (1986)).

FN8. The ECPA legislative history's explanation of the prohibitions regarding disclosure also persuades us of the soundness of Turk's interpretation of "intercept" and our understanding of the distinctions Congress intended to draw between communications being transmitted and communications in electronic storage. In describing Title II's prohibitions against disclosure of the contents of stored communications, the Senate Report points out that s 2702(a) (part of Title II) "generally prohibits the provider of a wire or electronic communication service to the public from knowingly divulging the contents of any communication while in electronic storage by that service to any person other

than the addressee or intended recipient." S.Rep. No. 99-541, 97th Cong. 2nd Sess. 37, 1986 U.S.C.C.A.N. 3555, 3591 (emphasis added). It then goes on to state that s 2511(3) of the Wiretap Act, as amended by Title I of the ECPA, "prohibits such a provider from divulging the contents of a communication while it is in transmission". Id. (emphasis added).

FN9. It goes without saying that we generally will not consider issues raised for the first time at oral argument. For this rare exception, the parties, as ordered, filed supplemental briefs on this point.

FN10. Section 2703 sets forth the requirements for governmental access to the contents of electronic (but not wire) communications. For electronic communications that have been in electronic storage for 180 days or less, the government can gain access to the contents pursuant to a federal or state warrant. 18 U.S.C. s 2703(a). For communications that are maintained by a remote computing service and that have been in storage for more than 180 days, the government can gain access by obtaining a warrant, by administrative or grand jury subpoena, or by obtaining a court order pursuant to s 2703(d). 18 U.S.C. s 2703(b). Section 2704 also deals only with electronic communications; it provides, inter alia, that a governmental entity may include in its subpoena or court order a requirement that the service provider create and maintain a duplicate of the contents of the electronic communications sought. 18 U.S.C. s 2704.

Bruce Sterling's Speech to the High Technology Crime Investigation Association - Lake Tahoe, Nov. 1994

Good morning, my name's Bruce Sterling, and I'm a sometime computer crime journalist and longtime science fiction writer from Austin Texas. I'm the guy who wrote HACKER CRACKDOWN, which is the book you're getting on one of those floppy disks that are being distributed at this gig like party favors.

People in law enforcement often ask me, Mr Sterling, if you're a science fiction writer like you say you are, then why should you care about American computer police and private security? And also, how come my kids can never find any copies of your sci-fi novels? Well, my publishers do their best. The truth of the matter is that I've survived my brief career as a computer-crime journalist. I'm now back to writing science fiction full time, like I want to do and like I ought to do. I really can't help the rest of it.

It's true that HACKER CRACKDOWN is still available on the stands at your friendly local bookstore --maybe a better chance if it's a computer bookstore. In fact it's in its second paperback printing, which is considered pretty good news in my business. The critics have been very kind about that book. But even though I'm sure I could write another book like HACKER CRACKDOWN every year for the rest of my life, I'm just not gonna do that.

Instead, let me show you some items out of this bag. This is HACKER CRACKDOWN, the paperback. And see, this is a book of my short stories that has come out since I published HACKER CRACKDOWN! And here's a brand new hardback novel of mine which came out just last month! Hard physical evidence of my career as a fiction writer! I know these wacko cyberpunk sci-fi books are of basically zero relevance to you guys, but I'm absurdly proud of them, so I just had to show them off.

So why did I write HACKER CRACKDOWN in the first place? Well, I figured that somebody ought to do it, and nobody else was willing, that's why. When I first got interested in Operation Sundevil and

the Legion of Doom and the raid on Steve Jackson Games and so forth, it was 1990. All these issues were very obscure. It was the middle of the Bush Administration. There was no information superhighway vice president. There was no WIRED magazine. There was no Electronic Frontier Foundation. There was no Clipper Chip and no Digital Telephony Initiative. There was no PGP and no World Wide Web. There were a few books around, and a couple of movies, that glamorized computer crackers, but there had never been a popular book written about American computer cops.

When I got started researching HACKER CRACKDOWN, my first and only nonfiction book, I didn't even think I was going to write any such book. There were four other journalists hot on the case who were all rather better qualified than I was. But one by one they all dropped out. Eventually I realized that either I was going to write it, or nobody was ever going to tell the story. All those strange events and peculiar happenings would have passed, and left no public record. I couldn't help but feel that if I didn't take the trouble and effort to tell people what had happened, it would probably all have to happen all over again. And again and again, until people finally noticed it and were willing to talk about it publicly.

Nowadays it's very different. There are about a million journalists with Internet addresses now. There are other books around, like for instance Hafner and Markoff's CYBERPUNK OUTLAWS AND HACKERS, which is a far better book about hackers than my book is. Mungo and Clough's book APPROACHING ZERO has a pretty interesting take on the European virus scene. Joshua Quittner has a book coming out on the Masters of Deception hacking group. Then there's this other very recent book I have here, CYBERSPACE AND THE LAW by Cavazos and Morin, which is a pretty good practical handbook on digital civil liberties issues. This book explains in pretty good legal detail exactly what kind of stunts with your modem are likely to get you into trouble. This is a useful service for keeping people out of hot water, which is pretty much what my book was intended to do, only this book does it better. And there have been a lot of magazine and newspaper articles published.

Basically, I'm no longer needed as a computer crime journalist. The world is full of computer journalists now, and the stuff I was writing about four years ago, is hot and sexy and popular now. That's why I don't have to write it any more. I was ahead of my time. I'm supposed to be ahead of my time. I'm a science fiction writer.

Believe it or not, I'm needed to write science fiction. Taking a science fiction writer and turning him into a journalist is like stealing pencils from a blind man's cup.

So frankly, I haven't been keeping up with you guys, and your odd and unusual world, with the same gusto I did in 90 and 91. Nowadays, I spend all my time researching science fiction. I spent most of 92 and 93 learning about tornadoes and the Greenhouse Effect. At the moment, I'm really interested in photography, cosmetics and computer interfaces. In 95 and 96 I'll be interested in something else. That may seem kind of odd and dilettantish on my part. It doesn't show much intellectual staying power. But my intellectual life doesn't have to make any sense. Because I'm a science fiction writer.

Even though I'm not in the computer crime game any more, I do maintain an interest. For a lot of pretty good reasons. I still read most of the computer crime journalism that's out there. And I'll tell you one thing about it. There's way, way too much blather about teenage computer intruders, and nowhere near enough coverage of computer cops. Computer cops are a hundred times more interesting than sneaky teenagers with kodes and kards. A guy like Carlton Fitzpatrick should be a hundred times more famous than some wretched hacker kid like Mark Abene. A group like the FCIC is a hundred times more influential and important and interesting than the Chaos Computer Club, Hack-Tic, and the 2600 group all put together.

The United States Secret Service is a heavy outfit. It's astounding how little has ever been written or published about Secret Service people, and their lives, and their history, and how life really looks to them. Cops are really good material for a journalist or a fiction writer. Cops see things most human beings never see. Even private security people have a lot to say for themselves. Computer-intrusion hackers and phone phreaks, by contrast, are basically pretty damned boring.

You know, I used to go actively looking for hackers, but I don't bother any more. I don't have to. Hackers come looking for me these days. And they find me, because I make no particular effort to hide. I get these phone calls -- I mean, I know a lot of you have gotten these hacker phone calls -- but for me they go a lot like this:

Ring ring. "Hello?"

"Is this Bruce Sterling?"

"Yeah, you got him."

"Are you the guy who wrote HACKER CRACKDOWN?"

"Yeah, that's me, dude. What's on your mind?"

"Uh, nothing -- I just wanted to know if you were there!"

"Well, okay, I'm here. If you ever get anything on your mind, you let me know." Click, buzz. I get dozens of calls like that.

And, pretty often, I'll get another call about 24 hours later, and it'll be the same kid, only this time he has ten hacker buddies with him on some illegal bridge call. They're the Scarlet Scorpion and the Electric Ninja and the Flaming Rutabaga, and they really want me to log onto their pirate bulletin board system, the Smurfs in Hell BBS somewhere in Wisconsin or Ohio or Idaho. I thank them politely for the invitation and I tell them I kind of have a lot of previous engagements, and then they leave me alone.

I also get a lot of call from journalists. Journalists doing computer crime stories. I've somehow acquired a reputation as a guy who knows something about computer crime and who is willing to talk to journalists. And I do that, too. Because I have nothing to lose. Why shouldn't I talk to another journalist? He's got a boss, I don't. He's got a deadline, I don't. I know more or less what I'm talking about, he usually doesn't have a ghost of a clue. And suppose I say something really rude or tactless or crazy, and it gets printed in public. So what? I'm a science fiction writer! What are they supposed to do to me -- take away my tenure?

Hackers will also talk to journalists. Hackers brag all the time. Computer cops, however, have not had a stellar record in their press relations. I think this is sad. I understand that there's a genuine need for operational discretion and so forth, but since a lot of computer cops are experts in telecommunications, you'd think they'd come up with some neat trick to get around these limitations.

Let's consider, for instance, the Kevin Mitnick problem. We all know who this guy Mitnick is. If you don't know who Kevin Mitnick is, raise your hand.... Right, I thought so. Kevin Mitnick is a hacker

and he's on the lam at the moment, he's a wanted fugitive. The FBI tried to nab Kevin a few months back at a computer civil liberties convention in Chicago and apprehended the wrong guy. That was pretty embarrassing, frankly. I was there, I saw it, I also saw the FBI trying to explain later to about five hundred enraged self-righteous liberals, and it was pretty sad. The local FBI office came a cropper because they didn't really know what Kevin Mitnick looked like.

I don't know what Mitnick looks like either, even though I've written about him a little bit, and my question is, how come? How come there's no publicly accessible WorldWideWeb page with mugshots of wanted computer-crime fugitives? Even the US Postal Service has got this much together, and they don't even have modems. Why don't the FBI and the USSS have public relations stations in cyberspace? For that matter, why doesn't the HTCIA have its own Internet site? All the computer businesses have Internet sites now, unless they're totally out of it. Why aren't computer cops in much, much better rapport with the computer community through computer networks? You don't have to grant live interviews with every journalist in sight if you don't want to, I can understand that that can create a big mess sometimes. But just put some data up in public, for heaven's sake. Crime statistics. Wanted posters. Security advice. Antivirus programs, whatever. Stuff that will help the cyberspace community that you are supposed to be protecting and serving.

I know there are people in computer law enforcement who are ready and willing and able to do this, but they can't make it happen because of too much bureaucracy and, frankly, too much useless hermetic secrecy. Computer cops ought to publicly walk the beat in cyberspace a lot more, and stop hiding your light under a bushel. What is your problem, exactly? Are you afraid somebody might find out that you exist?

I think that this is an amazing oversight and a total no-brainer on your part, to be the cops in an information society and not be willing to get online big-time and really push your information -- but maybe that's just me. I enjoy publicity, personally. I think it's good for people. I talk a lot, because I'm just an opinionated guy. I can't help it. A writer without an opinion is like a farmer without a plow, or a professor without a chalkboard, or a cop without a computer --it's just something basically useless and unnatural.

I don't mind talking to you this morning, I'm perfectly willing to talk to you, but since I'm not a cop or a prosecutor, I don't really have much of genuine nuts-and-bolts value to offer to you ladies and gentlemen. It's sheer arrogance on my part to lecture you on how to do your jobs. But since I was asked to come here, I can at least offer you my opinions. Since they're probably not worth much, I figure I ought to at least be frank about them.

First the good part. Let me tell you about a few recent events in your milieu that I have no conceptual difficulties with. Case in point. Some guy up around San Francisco is cloning off cellphones, and he's burning EPROMs and pirating cellular ID's, and he's moved about a thousand of these hot phones to his running buddies in the mob in Singapore, and they've bought him a real nice sports car with the proceeds. The Secret Service shows up at the guy's house, catches him with his little soldering irons in hand, busts him, hauls him downtown, calls a press conference after the bust, says that this activity is a big problem for cellphone companies and they're gonna turn up the heat on people who do this stuff. I have no problem with this situation. I even take a certain grim satisfaction in it. Is this a crime? Yes. Is this guy a bad guy with evil intent? Yes. Is law enforcement performing its basic duty here? Yes it is. Do I mind if corporate private security is kinda pitching in behind the scenes and protecting their own commercial interests here? No, not really. Is there some major civil liberties and free expression angle involved in this guy's ripping off cellular companies? No. Is there a threat to privacy here? Yeah -- him, the perpetrator. Is the Secret Service emptily boasting and grandstanding when they hang this guy out to dry in public? No, this looks like legitimate deterrence to me, and if they want a little glory out of it, well hell we all want a little glory sometimes. We can't survive without a little glory. Take the dumb bastard away with my blessing.

Okay, some group of Vietnamese Triad types hijack a truckload of chips in Silicon Valley, then move the loot overseas to the Asian black market through some smuggling network that got bored with running heroin. Are these guys "Robin Hoods of the Electronic Frontier?" I don't think so. Am I all impressed because some warlord in the Golden Triangle may be getting free computation services, and information wants to be free? No, this doesn't strike me as a positive development, frankly. Is organized crime a menace to our society? Yeah! It is!

I can't say I've ever had anything much to do --knowingly that is --with wiseguy types, but I spent a little time in Moscow recently, and in Italy too at the height of their Tangentopoly kickback scandal, and you know, organized crime and endemic corruption are very serious problems indeed. You get enough of that evil crap going on in your society and it's like nobody can breathe. A protection racket -- I never quite grasped how that worked and what it meant to victims, till I spent a couple of weeks in Moscow last December. That's a nasty piece of work, that stuff.

Another case. Some joker gets himself a job in a long distance provider, and he writes a PIN-trapping network program and he gets his mitts on about eight zillion PINs and he sells them for a buck apiece to his hacker buddies all over the US and Europe. Do I think this is clever? Yeah, it's pretty ingenious. Do I think it's a crime? Yes, I think this is a criminal act. I think this guy is basically corrupt. Do I think free or cheap long distance is a good idea? Yeah I do actually; I think if there were a very low flat rate on long distance, then you would see usage skyrocket so drastically that long distance providers would actually make more money in the long run. I'd like to see them try that experiment some time; I don't think the way they run phone companies in 1994 is the only possible way to run them successfully. I think phone companies are probably gonna have to change their act pretty drastically if they expect to survive in the 21st century's media environment.

But you know, that's not this guy's lookout. He's not the one to make that business decision. Theft is not an act of reform. He's abusing a position of trust as an employee in order to illegally line his own pockets. I think this guy is a crook.

So I have no problems with those recent law enforcement operations. I wish they'd gotten more publicity, and I'm kinda sorry that I wasn't able to give them more publicity myself, but at least I've heard of them, and I was paying some attention when they happened. Now I want to talk about some stuff that bugs me.

I'm an author and I'm interested in free expression, and it's only natural because that's my bailiwick. Free expression is a problem for writers, and it's always been a problem, and it's probably always gonna be a problem. We in the West have these ancient and honored tradition of Western free speech and freedom of the press, and in the US we have this rather more up-to-date concept of "freedom of

information." But even so, there is an enormous amount of "information" today which is highly problematic. Just because freedom of the press was in the Constitution didn't mean that people were able to stop thinking about what press-freedom really means in real life, and fighting about it and suing each other about it. We Americans have lots of problems with our freedom of the press and our freedom of speech. Problems like libel and slander. Incitement to riot. Obscenity. Child pornography. Flag-burning. Cross-burning. Race-hate propaganda. Political correctness. Sexist language. Mrs. Gore's Parents Music Resource Council. Movie ratings. Plagiarism. Photocopying rights. A journalist's so-called right to protect his sources. Fair-use doctrine. Lawyer-client confidentiality. Paid political announcements. Banning ads for liquor and cigarettes. The fairness doctrine for broadcasters. School textbook censors. National security. Military secrets. Industrial trade secrets. Arts funding for so-called obscenity. Even religious blasphemy such as Salman Rushdie's famous novel SATANIC VERSES, which is hated so violently by the kind of people who like to blow up the World Trade Center. All these huge problems about what people can say to each other, under what circumstances. And that's without computers and computer networks.

Every single one of those problems is applicable to cyberspace. Computers don't make any of these old free-expression problems go away; on the contrary, they intensify them, and they introduce a bunch of new problems. Problems like software piracy. Encryption. Wire-fraud. Interstate transportation of stolen digital property. Free expression on privately owned networks. So-called "data-mining" to invade personal privacy. Employers spying on employee e-mail. Intellectual rights over electronic publications. Computer search and seizure practice. Legal liability for network crashes. Computer intrusion, and on and on and on. These are real problems. They're out there. They're out there now. And in the future they're only going to get worse. And there's going to be a bunch of new problems that nobody's even imagined yet.

I worry about these issues because guys in a position like mine ought to worry about these issues. I can't say I've ever suffered much personally because of censorship, or through my government's objections to what I have to say. On the contrary, the current US government likes me so much that it kind of makes me nervous. But I've written ten books, and I don't think I've ever written a book that could have been legally published in its entirety fifty years

ago. Because my books talk about things that people just didn't talk about much fifty years ago, like sex for instance. In my books, my characters talk like normal people talk nowadays, which is to say that they cuss a lot. Even in HACKER CRACKDOWN there are sections where people use obscenities in conversations, and by the way the people I was quoting were computer cops.

I'm forty years old; I can remember when people didn't use the word "condom" in public. Nowadays, if you don't know what a condom is and how to use it, there's a pretty good chance you're gonna die. Standards change a lot. Culture changes a lot. The laws supposedly governing this behavior are very gray and riddled with contradictions and compromises. There are some people who don't want our culture to change, or they want to change it even faster in some direction they've got their own ideas about. When police get involved in cultural struggles it's always very highly politicized. The chances of its ending well are not good.

It's been quite a while since there was a really good ripping computer-intrusion scandal in the news. Nowadays the hotbutton issue is porn. Kidporn and other porn. I don't have much sympathy for kidporn people, I think the exploitation of children is a vile and grotesque criminal act, but I've seen some computer porn cases lately that look pretty problematic and peculiar to me. I don't think there's a lot to be gained by playing up the terrifying menace of porn on networks. Porn is just too treacherous an issue to be of much use to anybody. It's not a firm and dependable place in which to take a stand on how we ought to run our networks.

For instance, there's this Amateur Action case. We've got this guy and his wife in California, and they're selling some pretty seriously vile material off their bulletin board. They get indicted in Tennessee. What is that about? Do we really think that people in Memphis can enforce their pornographic community standards on people in California? I'd be genuinely impressed if a prosecutor got a jury in California to indict and convict some pornographer in Tennessee. I'd figure that Tennessee guy had to be some kind of pretty heavy-duty pornographer. Doing that in the other direction is like shooting fish in a barrel. There's something cheap about it. This doesn't smell like an airtight criminal case to me. This smells to me like some guy from Tennessee trying to enforce his own local cultural standards via a long-distance phone line. That may not be the actual truth about the case, but that's what the case looks like. It's real

hard to make a porn case look good at any time. If it's a weak case, then the prosecutor looks like a bluenosed goody-goody wimp. If it's a strong case, then the whole mess is so disgusting that nobody even wants to think about it or even look hard at the evidence. Porn is a no-win situation when it comes to the basic social purpose of instilling law and order on networks.

I think you could make a pretty good case in Tennessee that people in California are a bunch of flakey perverted lunatics, but I also think that in California you can make a pretty good case that people from Tennessee are a bunch of hillbilly fundamentalist wackos. You start playing off one community against another, pretty soon you're out of the realm of criminal law, and into the realm of trying to control people's cultural behavior with a nightstick. There's not a lot to be gained by this fight. You may intimidate a few pornographers here and there, but you're also likely to seriously infuriate a bunch of bystanders. It's not a fight you can win, even if you win a case, or two cases, or ten cases. People in California are never gonna behave in a way that satisfies people in Tennessee. People in California have more money and more power and more influence than people in Tennessee. People in California invented Hollywood and Silicon Valley, and people in Tennessee invented ways to put smut labels on rock and roll albums.

This is what Pat Buchanan and Newt Gingrich are talking about when they talk about cultural war in America. And this is what politically correct people talk about when they launch eighteen harassment lawsuits because some kid on some campus computer network said something that some ultrafeminist radical found demeaning. If I were a cop, I would be very careful of looking like a pawn in some cultural warfare by ambitious radical politicians. The country's infested with zealots now, zealots to the left and right. A lot of these people are fanatics motivated by fear and anger, and they don't care two pins about public order, or the people who maintain it and keep the peace in our society. They don't give a damn about justice, they have their own agendas. They'll seize on any chance they can get to make the other side shut up and knuckle under. They don't want a debate. They just want to crush their enemies by whatever means necessary. If they can use cops to do it, great! Cops are expendable.

There's another porn case that bugs me even more. There's this guy in Oklahoma City who had a big FidoNet bulletin board, and a storefront

where he sold CD-ROMs. Some of them, a few, were porn CD-ROMs. The Oklahoma City police catch this local hacker kid and of course he squeals like they always do, and he says don't nail me, nail this other adult guy, he's a pornographer. So off the police go to raid this guy's place of business, and while they're at it they carry some minicams and they broadcast their raid on that night's Oklahoma City evening news. This was a really high-tech and innovative thing to do, but it was also a really reckless cowboy thing to do, because it left no political fallback position. They were now utterly committed to crucifying this guy, because otherwise it was too much of a political embarrassment. They couldn't just shrug and say, "Well we've just busted this guy for selling a few lousy CD-ROMs that anybody in the country can mail-order with impunity out of the back of a computer magazine." They had to assemble a jury, with a couple of fundamentalist ministers on it, and show the most rancid graphic image files to the twelve good people and true. And you know, sure enough it was judged in a court to be pornography. I don't think there was much doubt that it was pornography, and I don't doubt that any jury in Oklahoma City would have called it pornography by the local Oklahoma City community standards. This guy got convicted. Lost the trial. Lost his business. Went to jail. His wife sued for divorce. He lost custody of his kids. He's a convict. His life is in ruins.

The hell of it, I don't think this guy was a pornographer by any genuine definition. He had no previous convictions. Never been in trouble, didn't have a bad character. Had an honorable war record in Vietnam. Paid his taxes. People who knew him personally spoke very highly of him. He wasn't some loony sleazebag. He was just a guy selling disks that other people just like him sell all over the country, without anyone blinking an eye. As far as I can figure it, the Oklahoma City police and an Oklahoma prosecutor skinned this guy and nailed his hide to the side of a barn, just because they didn't want to look bad. I think a serious injustice was done here.

I also think it was a terrible public relations move. There's a magazine out called BOARDWATCH, practically everybody who runs a bulletin board system in this country reads it. When the editor of this magazine heard about the outcome of this case, he basically went nonlinear. He wrote this scorching furious editorial berating the authorities. The Oklahoma City prosecutor sent his little message all right, and it went over the Oklahoma City evening news, and probably made him look pretty good, locally, personally. But this magazine sent a much bigger and much angrier message, which went all

over the country to a perfect target computer-industry audience of BBS sysops. This editor's message was that the Oklahoma City police are a bunch of crazed no-neck gestapo, who don't know nothing about nothing, and hate anybody who does. I think that the genuine cause of computer law and order was very much harmed by this case.

It seems to me that there are a couple of useful lessons to be learned here. The first, of course, is don't sell porn in Oklahoma City. And the second lesson is, if your city's on an antiporn crusade and you're a cop, it's a good idea to drop by the local porn outlets and openly tell the merchants that porn is illegal. Tell them straight out that you know they have some porn, and they'd better knock it off. If they've got any sense, they'll take this word from the wise and stop breaking the local community standards forthwith. If they go on doing it, well, presumably they're hardened porn merchants of some kind, and when they get into trouble with ambitious local prosecutors they'll have no one to blame but themselves. Don't jump in headfirst with an agenda and a videocam. Because it's real easy to wade hip deep into a blaze of publicity, but it's real hard to wade back out without getting the sticky stuff all over you.

Well, it's generally a thankless lot being an American computer cop. You know this, I know this. I even regret having to bring these matters up, though I feel that I ought to, given the circumstances. I do, however, see one large ray of light in the American computer law enforcement scene, and that is the behavior of computer cops in other countries. American computer cops have had to suffer under the spotlights because they were the first people in the world doing this sort of activity. But now we're starting to see other law enforcement people weighing in in other countries. To judge by early indications, the situation's going to be a lot worse overseas.

Italy, for instance. The Italian finance police recently decided that everybody on FidoNet was a software pirate, so they went out and seized somewhere between fifty and a hundred bulletin boards. Accounts are confused, not least because most of the accounts are in Italian. Nothing much has appeared in the way of charges or convictions, and there's been a lot of anguished squawling from deeply alienated and radicalized Italian computer people. Italy is a country where entire political parties have been annihilated because of endemic corruption and bribery scandals. A country where organized crime shoots judges and blows up churches with car bombs. They got a guy running the country now who is basically Ted Turner in Italian

drag --he owns a bunch of television stations -- and here his federal cops have gone out and busted a bunch of left-wing bulletin board systems. It's not doing much good for the software piracy problem and it's sure not helping the local political situation. In Italy politics are so weird that the Italian Communist Party has a national reputation as the party of honest government. The Communists hate the guts of this new Prime Minister, and he's in bed with the neo-fascist ultra-right and a bunch of local ethnic separatists who want to cut the country in half. That's a very strange and volatile scene.

The hell of it is, in the long run I think the Italians are going to turn out to be one of the better countries at handling computer crime. Wait till we start hearing from the Poles, the Romanians, the Chinese, the Serbs, the Turks, the Pakistanis, the Saudis.

Here in America we're actually getting used to this stuff, a little bit, sort of. We have a White House with its own Internet address and its own World Wide Web page. Owning and using a modem is fashionable in the USA. American law enforcement agencies are increasingly equipped with a clue. In Europe you have computers all over the place, but they are imbedded in a patchwork of PTTs and peculiar local jurisdictions and even more peculiar and archaic local laws. I think the chances of some social toxic reaction from computing and telecommunications are much higher in Europe and Asia than in the USA. I think that in a few more years, American cops are going to earn a global reputation as being very much on top of this stuff. I think there's a fairly good chance that the various interested parties in the USA can find some kind of workable accommodation and common ground on most of the important social issues. There won't be so much blundering around, not so many unpleasant surprises, not so much panic and hysteria.

As for the computer crime scene, I think it's pretty likely that American computer crime is going to look relatively low-key, compared to the eventual rise of ex-Soviet computer crime, and Eastern European computer crime, and Southeast Asian computer crime.

I'm a science fiction writer, and I like to speculate about the future. I think American computer police are going to have a hard row to hoe, because they are almost always going to be the first in the world to catch hell from these issues. Certain bad things are naturally going to happen here first, because we're the people who are

inventing almost all the possibilities. But I also feel that it's not very likely that bad things will reach their full extremity of awfulness here. It's quite possible that American computer police will make some really awful mistakes, but I can almost guarantee that other people's police will make mistakes worse by an order of magnitude. American police may hit people with sticks, but other people's police are going to hit people with axes and cattle prods. Computers will probably help people manage better in those countries where people can actually manage. In countries that are falling apart, overcrowded countries with degraded environments and deep social problems, computers might well make things fall apart even faster.

Countries that have offshore money-laundries are gonna have offshore data laundries. Countries that now have lousy oppressive governments and smart, determined terrorist revolutionaries, are gonna have lousy oppressive governments and smart determined terrorist revolutionaries with computers. Not too long after that, they're going to have tyrannical revolutionary governments run by zealots with computers, and then we're likely to see just how close to Big Brother a government can really get. Dealing with these people is going to be a big problem for us.

Other people have worse problems than we do, and I suppose that's some comfort to us in a way. But we've got our problems here, too. It's no use hiding from them. Since 1980 the American prison population has risen by one hundred and eighty eight percent. In 1993 we had 948,881 prisoners in federal or state correctional facilities. I appreciate the hard work it took to put these nearly one million people into American prisons, but you know, I can't say that the knowledge that there are a million people in prison in my country really makes me feel much safer. Quite the contrary, really. Does it make keeping public order easier when there are so many people around with no future and no stake in the status quo and nothing left to lose? I don't think it does.

We've got a governor's race in my state that's a nasty piece of work -- the incumbent and the challenger are practically wrestling in public for the privilege of putting on a black hood and jabbing people with the needle. That's not a pretty sight. I hear a lot about vengeance and punishment lately, but I don't hear a lot about justice. I hear a lot about rights and lawsuits, but I don't hear a lot about debate and public goodwill and public civility. I think

it's past time in this country that we stopped demonizing one another, and tried to see each other as human beings and listen seriously to each other. And personally, I think I've talked enough this morning. It's time for me to listen to you guys for a while.

I confess that in my weaker moments I've had the bad taste to become a journalist. But I didn't come here to write anything about you, I've given that up for now. I'm here as a citizen and an interested party. I was glad to be invited to come here, because I was sure I'd learn something that I ought to know. I appreciate your patience and attention very much, and I hope you'll see that I mean to return the favor. Thanks. Thanks a lot.

CHILLING EFFECT OF BBS RAIDS ON ELECTRONIC SPEECH

Has the recent series of raids against BBS operators had a "chilling effect" - that is, has it caused BBS owners and users to `censor' their OWN speech out of fear of retaliation?

This "code of standards," adopted by a large users' group, in Washington DC, seems to show a definite chilling effect on their BBS speech. This was downloaded from USENET alt.bbs.

We do not present this "code of standards" as something to be imitated, but as an example of government interference with free speech . . . through fear.

Capitol PC Users Group Minimum Code of Standards

SCOPE:
This Minimum Code of Standards applies to both users and SYStem Operators (SYSOPs) of electronic bulletin boards available to the general public.

FREEDOM OF SPEECH AND IDEAS
Each user and SYSOP of such systems shall actively encourage and promote the free exchange and discussion of information, ideas, and opinions, except when the content would:

- Compromise the national security of the United States.
- violate proprietary rights.
- violate personal privacy,
- constitute a crime,
- constitute libel, or
- violate applicable state, federal or local laws and regulations affecting telecommunications.

DISCLOSURE
Each user and SYSOP of such system will:

- disclose their real name, and
- fully disclose any personal, financial, or commercial interest when evaluating any specific product or service.

PROCEDURES
SYSOPS shall:

- review in a timely manner all publicly accessible information, and
- delete any information which they know or should know conflicts with this code of standards.

A 'timely manner' is defined as what is reasonable based on the potential harm that could be expected. Users are responsible for:

- ensuring that any information they transmit to such systems adheres to this Minimum Code of Standards, and
- upon discovering violations of the Minimum Code of Standards, notifying the SYSOP immediately.

IMPLEMENTATION

Electronic bulletin board systems that choose to follow this Minimum Code of Standards shall notify their users by publishing this Minimum Code, as adopted by the [Capitol PC Users Group], and prominently display the following:

'This system subscribes to the Capitol PC Users Group Minimum Code of Standards for electronic bulletin board systems.'

CRIME AND PUZZLEMENT

by John Perry Barlow
barlow@well.sf.ca.us

Desperados of the DataSphere

So me and my sidekick Howard, we was sitting out in front of the 40 Rod Saloon one evening when he all of a sudden says, "Lookee here. What do you reckon?" I look up and there's these two strangers riding into town. They're young and got kind of a restless, bored way about 'em. A person don't need both eyes to see they mean trouble...

Well, that wasn't quite how it went. Actually, Howard and I were floating blind as cave fish in the electronic barrens of the WELL, so the whole incident passed as words on a display screen:

Howard: Interesting couple of newusers just signed on. One calls himself acid and the other's optik.

Barlow: Hmmm. What are their real names?

Howard: Check their finger files.

And so I typed !finger acid. Several seconds later the WELL's Sequent computer sent the following message to my Macintosh in Wyoming:

Login name: acid In real life: Acid Phreak

By this, I knew that the WELL had a new resident and that his corporeal analog was supposedly called Acid Phreak. Typing !finger optik yielded results of similar insufficiency, including the claim that someone, somewhere in the real world, was walking around calling himself Phiber Optik. I doubted it.

However, associating these sparse data with the knowledge that the WELL was about to host a conference on computers and security rendered the conclusion that I had made my first sighting of genuine computer crackers. As the arrival of an outlaw was a major event to the settlements of the Old West, so was the appearance of crackers cause for stir on the WELL.

The WELL (or Whole Earth 'Lectronic Link) is an example of the latest thing in frontier villages, the computer bulletin board. In this kind of small town, Main Street is a central minicomputer to which

(in the case of the WELL) as many as 64 microcomputers may be connected at one time by phone lines and little blinking boxes called modems.

In this silent world, all conversation is typed. To enter it, one forsakes both body and place and becomes a thing of words alone. You can see what your neighbors are saying (or recently said), but not what either they or their physical surroundings look like. Town meetings are continuous and discussions rage on everything from sexual kinks to depreciation schedules.

There are thousands of these nodes in the United States, ranging from PC clone hamlets of a few users to mainframe metros like CompuServe, with its 550,000 subscribers. They are used by corporations to transmit memoranda and spreadsheets, universities to disseminate research, and a multitude of factions, from apiarists to Zoroastrians, for purposes unique to each.

Whether by one telephonic tendril or millions, they are all connected to one another. Collectively, they form what their inhabitants call the Net. It extends across that immense region of electron states, microwaves, magnetic fields, light pulses and thought which sci-fi writer William Gibson named Cyberspace.

Cyberspace, in its present condition, has a lot in common with the 19th Century West. It is vast, unmapped, culturally and legally ambiguous, verbally terse (unless you happen to be a court stenographer), hard to get around in, and up for grabs. Large institutions already claim to own the place, but most of the actual natives are solitary and independent, sometimes to the point of sociopathy. It is, of course, a perfect breeding ground for both outlaws and new ideas about liberty.

Recognizing this, Harper's Magazine decided in December, 1989 to hold one of its periodic Forums on the complex of issues surrounding computers, information, privacy, and electronic intrusion or "cracking." Appropriately, they convened their conference in Cyberspace, using the WELL as the "site."

Harper's invited an odd lot of about 40 participants. These included: Clifford Stoll, whose book The Cuckoo's Egg details his cunning efforts to nab a German cracker. John Draper or "Cap'n Crunch," the grand-daddy of crackers whose blue boxes got Wozniak and Jobs into consumer electronics. Stewart Brand and Kevin Kelly of Whole Earth fame. Steven Levy, who wrote the seminal Hackers. A retired Army colonel named Dave Hughes. Lee Felsenstein, who designed the Osborne computer and was once called the "Robespierre of computing." A UNIX wizard and former hacker named Jeff

Poskanzer. There was also a score of aging techno-hippies, the crackers, and me.

What I was doing there was not precisely clear since I've spent most of my working years either pushing cows or song-mongering, but I at least brought to the situation a vivid knowledge of actual cow-towns, having lived in or around one most of my life.

That and a kind of innocence about both the technology and morality of Cyberspace which was soon to pass into the confusion of knowledge.

At first, I was inclined toward sympathy with Acid 'n' Optik as well as their colleagues, Adelaide, Knight Lightning, Taran King, and Emmanuel. I've always been more comfortable with outlaws than Republicans, despite having more certain credentials in the latter camp.

But as the Harper's Forum mushroomed into a boom-town of ASCII text (the participants typing 110,000 words in 10 days), I began to wonder. These kids were fractious, vulgar, immature, amoral, insulting, and too damned good at their work.

Worse, they inducted a number of former kids like myself into Middle Age. The long feared day had finally come when some gunsel would yank my beard and call me, too accurately, an old fart.

Under ideal circumstances, the blind gropings of bulletin board discourse force a kind of Noh drama stylization on human commerce. Intemperate responses, or "flames" as they are called, are common even among conference participants who understand one another, which, it became immediately clear, the cyberpunks and techno-hippies did not.

My own initial enthusiasm for the crackers wilted under a steady barrage of typed testosterone. I quickly remembered I didn't know much about who they were, what they did, or how they did it. I also remembered stories about crackers working in league with the Mob, ripping off credit card numbers and getting paid for them in (stolen) computer equipment.

And I remembered Kevin Mitnik. Mitnik, now 25, recently served federal time for a variety of computer and telephone related crimes. Prior to incarceration, Mitnik was, by all accounts, a dangerous guy with a computer. He disrupted phone company operations and arbitrarily disconnected the phones of celebrities. Like the kid in Wargames, he broke into the North American Defense Command computer in Colorado Springs.

Unlike the kid in Wargames, he is reputed to have made a practice of destroying and altering data. There is even the (perhaps apocryphal) story that he altered the credit information of his probation officer and other enemies. Digital Equipment claimed that his depredations cost them more than $4 million in computer downtime and file rebuilding. Eventually, he was turned in by a friend who, after careful observation, had decided he was "a menace to society."

His spectre began to hang over the conference. After several days of strained diplomacy, the discussion settled into a moral debate on the ethics of security and went critical.

The techno-hippies were of the unanimous opinion that, in Dylan's words, one "must be honest to live outside the law." But these young strangers apparently lived by no code save those with which they unlocked forbidden regions of the Net.

They appeared to think that improperly secured systems deserved to be violated and, by extension, that unlocked houses ought to be robbed. This latter built particular heat in me since I refuse, on philosophical grounds, to lock my house.

Civility broke down. We began to see exchanges like:

Dave Hughes: Clifford Stoll said a wise thing that no one has commented on. That networks are built on trust. If they aren't, they should be.

Acid Phreak: Yeah. Sure. And we should use the 'honor system' as a first line of security against hack attempts.

Jef Poskanzer: This guy down the street from me sometimes leaves his back door unlocked. I told him about it once, but he still does it. If I had the chance to do it over, I would go in the back door, shoot him, and take all his money and consumer electronics. It's the only way to get through to him.

Acid Phreak: Jef Poskanker (Puss? Canker? yechh) Anyway, now when did you first start having these delusions where computer hacking was even *remotely* similar to murder?

Presented with such a terrifying amalgam of raw youth and apparent power, we fluttered like a flock of indignant Babbitts around the Status Quo, defending it heartily. One former hacker howled to the Harper's editor in charge of the forum, "Do you or do you not have names and addresses for these criminals?" Though they had committed no obvious crimes, he was ready to call the police.

They finally got to me with:

Acid: Whoever said they'd leave the door open to their house... where do you live? (the address) Leave it to me in mail if you like.

I had never encountered anyone so apparently unworthy of my trust as these little nihilists. They had me questioning a basic tenet, namely that the greatest security lies in vulnerability. I decided it was time to put that principal to the test...

Barlow: Acid. My house is at 372 North Franklin Street in Pinedale, Wyoming. If you're heading north on Franklin, you go about two blocks off the main drag before you run into hay meadow on the left. I've got the last house before the field. The computer is always on...

And is that really what you mean? Are you merely just the kind of little sneak that goes around looking for easy places to violate? You disappoint me, pal. For all your James Dean-On-Silicon rhetoric, you're not a cyberpunk. You're just a punk.

Acid Phreak: Mr. Barlow: Thank you for posting all I need to get your credit information and a whole lot more! Now, who is to blame? ME for getting it or YOU for being such an idiot?! I think this should just about sum things up.

Barlow: Acid, if you've got a lesson to teach me, I hope it's not that it's idiotic to trust one's fellow man. Life on those terms would be endless and brutal. I'd try to tell you something about conscience, but I'd sound like Father O'Flannigan trying to reform the punk that's about to gutshoot him. For no more reason that to watch him die.

But actually, if you take it upon yourself to destroy my credit, you might do me a favor. I've been looking for something to put the brakes on my burgeoning materialism.

I spent a day wondering whether I was dealing with another Kevin Mitnik before the other shoe dropped:

Barlow: ... With crackers like acid and optik, the issue is less intelligence than alienation. Trade their modems for skateboards and only a slight conceptual shift would occur.

Optik: You have some pair of balls comparing my talent with that of a skateboarder. Hmmm... This was indeed boring, but nonetheless:

At which point he downloaded my credit history.

Optik had hacked the core of TRW, an institution which has made my business (and yours) their business, extracting from it an abbreviated (and incorrect) version of my personal financial life. With this came the implication that he and Acid could and would revise it to my disadvantage if I didn't back off.

I have since learned that while getting someone's TRW file is fairly trivial, changing it is not. But at that time, my assessment of the crackers' black skills was one of superstitious awe. They were digital brujos about to zombify my economic soul.

To a middle-class American, one's credit rating has become nearly identical to his freedom. It now appeared that I was dealing with someone who had both the means and desire to hoodoo mine, leaving me trapped in a life of wrinkled bills and money order queues. Never again would I call the Sharper Image on a whim.

I've been in redneck bars wearing shoulder-length curls, police custody while on acid, and Harlem after midnight, but no one has ever put the spook in me quite as Phiber Optik did at that moment. I realized that we had problems which exceeded the human conductivity of the WELL's bandwidth. If someone were about to paralyze me with a spell, I wanted a more visceral sense of him than could fit through a modem.

I e-mailed him asking him to give me a phone call. I told him I wouldn't insult his skills by giving him my phone number and, with the assurance conveyed by that challenge, I settled back and waited for the phone to ring. Which, directly, it did.

In this conversation and the others that followed I encountered an intelligent, civilized, and surprisingly principled kid of 18 who sounded, and continues to sound, as though there's little harm in him to man or data. His cracking impulses seemed purely exploratory, and I've begun to wonder if we wouldn't also regard spelunkers as desperate criminals if AT&T owned all the caves.

The terrifying poses which Optik and Acid had been striking on screen were a media-amplified example of a human adaptation I'd seen before: One becomes as he is beheld. They were simply living up to what they thought we, and, more particularly, the editors of Harper's, expected of them. Like the televised tears of disaster victims, their snarls adapted easily to mass distribution.

Months later, Harper's took Optik, Acid and me to dinner at a Manhattan restaurant which, though very fancy, was appropriately Chinese. Acid and Optik, as material beings, were well-scrubbed and fashionably-clad. They looked to be dangerous as ducks. But, as Harper's and the rest of the media have discovered to their delight, the boys had developed distinctly showier personae for their rambles through the howling wilderness of Cyberspace.

Glittering with spikes of binary chrome, they strode past the kleig lights and into the digital distance. There they would be outlaws. It was only a matter of time before they started to believe themselves as bad as they sounded. And no time at all before everyone else did.

In this, they were like another kid named Billy, many of whose feral deeds in the pre-civilized West were encouraged by the same dime novelist who chronicled them. And like Tom Horn, they seemed to have some doubt as to which side of the law they were on. Acid even expressed an ambition to work for the government someday, nabbing "terrorists and code abusers."

There is also a frontier ambiguity to the "crimes" the crackers commit. They are not exacdly stealing VCR's. Copying a text file from TRW doesn't deprive its owner of anything except informational exclusivity. (Though it may said that information has monetary value only in proportion to its containment.)

There was no question that they were making unauthorized use of data channels. The night I met them, they left our restaurant table and disappeared into the phone booth for a long time. I didn't see them marshalling quarters before they went.

And, as I became less their adversary and more their scoutmaster, I began to get "conference calls" in which six or eight of them would crack pay phones all over New York and simultaneously land on my line in Wyoming. These deft maneuvers made me think of skydiving stunts where large groups convene geometrically in free fall. In this case, the risk was largely legal.

Their other favorite risky business is the time-honored adolescent sport of trespassing. They insist on going where they don't belong. But then teen-age boys have been proceeding uninvited since the dawn of human puberty. It seems hard-wired. The only innovation is in the new form of the forbidden zone the means of getting in it.

In fact, like Kevin Mitnik, I broke into NORAD when I was 17. A friend and I left a nearby "woodsie" (as rustic adolescent drunks were called in Colorado) and tried to get inside the Cheyenne

Mountain. The chrome-helmeted Air Force MP's held us for about 2 hours before letting us go. They weren't much older than us and knew exactly our level of national security threat. Had we come cloaked in electronic mystery, their alert status certainly would have been higher.

Whence rises much of the anxiety. Everything is so ill-defined. How can you guess what lies in their hearts when you can't see their eyes? How can one be sure that, like Mitnik, they won't cross the line from trespassing into another adolescent pastime, vandalism? And how can you be sure they pose no threat when you don't know what a threat might be?

And for the crackers some thrill is derived from the metamorphic vagueness of the laws themselves. On the Net, their effects are unpredictable. One never knows when they'll bite.

This is because most of the statutes invoked against the crackers were designed in a very different world from the one they explore. For example, can unauthorized electronic access can be regarded as the ethical equivalent of old-fashioned trespass? Like open range, the property boundaries of Cyberspace are hard to stake and harder still to defend.

Is transmission through an otherwise unused data channel really theft? Is the track-less passage of a mind through TRW's mainframe the same as the passage of a pickup through my Back 40? What is a place if Cyberspace is everywhere? What are data and what is free speech? How does one treat property which has no physical form and can be infinitely reproduced? Is a computer the same as a printing press? Can the history of my business affairs properly belong to someone else? Can anyone morally claim to own knowledge itself?

If such questions were hard to answer precisely, there are those who are ready to try. Based on their experience in the Virtual World, they were about as qualified to enforce its mores as I am to write the Law of the Sea. But if they lacked technical sophistication, they brought to this task their usual conviction. And, of course, badges and guns.

******

Operation Sun Devil

"Recently, we have witnessed an alarming number of young people who, for a variety of sociological and psychological reasons, have become attached to their computers and are exploiting their potential in a criminal manner. Often, a progression of criminal activity occurs which involves

telecommunications fraud (free long distance phone calls), unauthorized access to other computers (whether for profit, fascination, ego, or the intellectual challenge), credit card fraud (cash advances and unauthorized purchases of goods), and then move on to other destructive activities like computer viruses."

"Our experience shows that many computer hacker suspects are no longer misguided teenagers mischievously playing games with their computers in their bedrooms. Some are now high tech computer operators using computers to engage in unlawful conduct."
-- Excerpts from a statement by Garry M. Jenkins
    Asst. Director, U. S. Secret Service

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue but upon probable cause, support by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."
-- Amendment IV, United States Constitution

On January 24, 1990, a platoon of Secret Service agents entered the apartment which Acid Phreak shares with his mother and 12 year-old sister. The latter was the only person home when they burst through the door with guns drawn. They managed to hold her at bay for about half an hour until their quarry happened home.

By then, they were nearly done packing up Acid's worldly goods, including his computer, his notes (both paper and magnetic), books, and such dubiously dangerous tools as a telephone answering machine, a ghetto blaster and his complete collection of audio tapes. One agent asked him to define the real purpose of the answering machine and was frankly skeptical when told that it answered the phone. The audio tapes seemed to contain nothing but music, but who knew what dark data Acid might have encoded between the notes...

When Acid's mother returned from work, she found her apartment a scene of apprehended criminality. She asked what, exactly, her son had done to deserve all this attention and was told that, among other things, he had caused the AT&T system crash several days earlier. (Previously AT&T had taken full responsibility.) Thus, the agent explained, her darling boy was thought to have caused over a billion dollars in damage to the economy of the United States.

This accusation was never turned into a formal charge. Indeed, no charge of any sort of was filed against Mr. Phreak then and, although the Secret Service maintained resolute possession of his hardware, software, and data, no charge had been charged 4 months later.

Across town, similar scenes were being played out at the homes of Phiber Optik and another colleague code-named Scorpion. Again, equipment, notes, disks both hard and soft, and personal effects were confiscated. Again no charges were filed.

Thus began the visible phase of Operation Sun Devil, a two-year Secret Service investigation which involved 150 federal agents, numerous local and state law enforcement agencies. and the combined security resources of PacBell, AT&T, Bellcore, Bell South MCI, U.S. Sprint, Mid-American, Southwestern Bell, NYNEX, U.S. West and American Express.

The focus of this impressive institutional array was the Legion of Doom, a group which never had any formal membership list but was thought by the members with whom I spoke to number less than 20, nearly all of them in their teens or early twenties.

I asked Acid why they'd chosen such a threatening name. "You wouldn't want a fairy kind of thing like Legion of Flower Pickers or something. But the media ate it up too. Probing the Legion of Doom like it was a gang or something, when really it was just a bunch of geeks behind terminals."

******

Sometime in December 1988, a 21 year-old Atlanta-area Legion of Doomster named The Prophet cracked a Bell South computer and downloaded a three-page text file which outlined, in bureaucrat-ese of surpassing opacity, the administrative procedures and responsibilities for marketing, servicing, upgrading, and billing for Bell South's 911 system.

A dense thicket of acronyms, the document was filled with passages like:

"In accordance with the basic SSC/MAC strategy for provisioning, the SSC/MAC will be Overall Control Office (OCO) for all Notes to PSAP circuits (official services) and any other services for this customer. Training must be
scheduled for all SSC/MAC involved personnel during the pre-service stage of the project."

And other such.

At some risk, I too have a copy of this document. To read the whole thing straight through without entering coma requires either a machine or a human who has too much practice thinking like one. Anyone who can understand it fully and fluidly has altered his consciousness beyond the ability to ever again read Blake, Whitman, or Tolstoy. It is, quite simply, the worst writing I have ever tried to read.

Since the document contains little of interest to anyone who is not a student of advanced organizational sclerosis...that is, no access codes, trade secrets, or proprietary information...I assume The Prophet only copied this file as a kind of hunting trophy. He had been to the heart of the forest and had returned with this coonskin to nail to the barn door.

Furthermore, he was proud of his accomplishment, and since such trophies are infinitely replicable, he wasn't content to nail it to his door alone. Among the places he copied it was a UNIX bulletin board (rather like the WELL) in Lockport, Illinois called Jolnet.

It was downloaded from there by a 20 year-old hacker and pre-law student (whom I had met in the Harper's Forum) who called himself Knight Lightning. Though not a member of the Legion of Doom, Knight Lightning and a friend, Taran King, also published from St. Louis and his fraternity house at the University of Missouri a worldwide hacker's magazine called Phrack. (From phone phreak and hack.)

Phrack was an unusual publication in that it was entirely virtual. The only time its articles hit paper was when one of its subscribers decided to print out a hard copy. Otherwise, its editions existed in Cyberspace and took no physical form.

When Knight Lightning got hold of the Bell South document, he thought it would amuse his readers and reproduced it in the next issue of Phrack. He had little reason to think that he was doing something illegal. There is nothing in it to indicate that it contains proprietary or even sensitive information. Indeed, it closely resembles telco reference documents which have long been publicly available.

However, Rich Andrews, the systems operator who oversaw the operation of Jolnet, thought there might be something funny about the document when he first ran across it in his system. To be on the safe side, he forwarded a copy of it to AT&T officials. He was subsequently contacted by the authorities, and he cooperated with them fully. He would regret that later.

On the basis of the forgoing, a Grand Jury in Lockport was persuaded by the Secret Service in early February to hand down a seven count indictment against The Prophet and Knight Lightning, charging them, among other things, with interstate transfer of stolen property worth more than $5,000. When The Prophet and two of his Georgia colleagues were arrested on February 7, 1990, the Atlanta papers reported they faced 40 years in prison and a $2 million fine. Knight Lightning was arrested on February 15.

The property in question was the affore-mentioned blot on the history of prose whose full title was A Bell South Standard Practice

(BSP) 660-225-104SV-Control Office Administration of Enhanced 911 Services for Special Services and Major Account Centers, March, 1988.

And not only was this item worth more than $5,000.00, it was worth, according to the indictment and Bell South, precisely $79,449.00. And not a penny less. We will probably never know how this figure was reached or by whom, though I like to imagine an appraisal team consisting of Franz Kafka, Joseph Heller, and Thomas Pynchon...

In addition to charging Knight Lightning with crimes for which he could go to jail 30 years and be fined $122,000.00, they seized his publication, Phrack, along with all related equipment, software and data, including his list of subscribers, many of whom would soon lose their computers and data for the crime of appearing on it.

I talked to Emmanuel Goldstein, the editor of 2600, another hacker publication which has been known to publish purloined documents. If they could shut down Phrack, couldn't they as easily shut down 2600?

He said, "I've got one advantage. I come out on paper and the Constitution knows how to deal with paper."

In fact, nearly all publications are now electronic at some point in their creation. In a modern newspaper, stories written at the scene are typed to screens and then sent by modem to a central computer. This computer composes the layout in electronic type and the entire product transmitted electronically to the presses. There, finally, the bytes become ink.

Phrack merely omitted the last step in a long line of virtual events. However, that omission, and its insignificant circulation, left it vulnerable to seizure based on content. If the 911 document had been the Pentagon Papers (another proprietary document) and Phrack the New York Times, a completion of the analogy would have seen the government stopping publication of the Times and seizing its every material possession, from notepads to presses.

Not that anyone in the newspaper business seemed particularly worried about such implications. They, and the rest of the media who bothered to report Knight Lightning's arrest were too obsessed by what they portrayed as actual disruptions of emergency service and with marvelling at the sociopathy of it. One report expressed relief that no one appeared to have died as a result of the "intrusions."

Meanwhile, in Baltimore, the 911 dragnet snared Leonard Rose, aka Terminus. A professional computer consultant who specialized in UNIX, Rose got a visit from the government early in February. The G-men forcibly detained his wife and children for six hours while

they interrogated Rose about the 911 document and ransacked his system.

Rose had no knowledge of the 911 matter. Indeed, his only connection had been occasional contact with Knight Lightning over several years...and admitted membership in the Legion of Doom. However, when searching his hard disk for 911 evidence, they found something else. Like many UNIX consultants, Rose did have some UNIX source code in his possession. Furthermore, there was evidence that he had transmitted some of it to Jolnet and left it there for another consultant.

UNIX is a ubiquitous operating system, and though its main virtue is its openness to amendment at the source level, it is nevertheless the property of AT&T. What had been widely distributed within businesses and universities for years was suddenly, in Rose's hands, a felonious possession.

Finally, the Secret Service rewarded the good citizenship of Rich Andrews by confiscating the computer where Jolnet had dwelt, along with all the e-mail, read and un-read, which his subscribers had left there. Like the many others whose equipment and data were taken by the Secret Service subsequently, he wasn't charged with anything. Nor is he likely to be. They have already inflicted on him the worst punishment a nerd can suffer: data death.

Andrews was baffled. "I'm the one that found it, I'm the one that turned it in...And I'm the one that's suffering," he said.

One wonders what will happen when they find such documents on the hard disks of CompuServe. Maybe I'll just upload my copy of Bell South Standard Practice (BSP) 660-225-104SV and see...

In any case, association with stolen data is all the guilt you need. It's quite as if the government could seize your house simply because a guest left a stolen VCR in an upstairs bedroom closet. Or confiscate all the mail in a post office upon finding a stolen package there. The first concept of modern jurisprudence to have arrived in Cyberspace seems to have been Zero Tolerance.

******

Rich Andrews was not the last to learn about the Secret Service's debonair new attitude toward the 4th Amendment's protection against unreasonable seizure.

Early on March 1, 1990, the offices of a role-playing game publisher in Austin, Texas called Steve Jackson Games were visited by agents of

the United States Secret Service. They ransacked the premises, broke into several locked filing cabinets (damaging them irreparably in the process) and eventually left carrying 3 computers, 2 laser printers, several hard disks, and many boxes of paper and floppy disks.

Later in the day, callers to the Illuminati BBS (which Steve Jackson Games operated to keep in touch with roll-players around the country) encountered the following message:

"So far we have not received a clear explanation of what the Secret Service was looking for, what they expected to find, or much of anything else. We are fairly certain that Steve Jackson Games is not the target of whatever investigation is being conducted; in any case, we have done nothing illegal and have nothing whatsoever to hide. However, the equipment that was seized is apparently considered to be evidence in whatever they're investigating, so we aren't likely to get it back any time soon. It could be a
month, it could be never."

It's been three months as I write this and, not only has nothing been returned to them, but, according to Steve Jackson, the Secret Service will no longer take his calls. He figures that, in the months since the raid, his little company has lost an estimated $125,000. With such a fiscal hemorrhage, he can't afford a lawyer to take after the Secret Service. Both the state and national offices of the ACLU told him to "run along" when he solicited their help.

He tried to go to the press. As in most other cases, they were unwilling to raise the alarm. Jackson theorized, "The conservative press is taking the attitude that the suppression of evil hackers is a good thing and that anyone who happens to be put out of business in the meantime...well, that's just their tough luck."

In fact, Newsweek did run a story about the event, portraying it from Jackson's perspective, but they were almost alone in dealing with it.

What had he done to deserve this nightmare? Role-playing games, of which Dungeons and Dragons is the most famous, have been accused of creating obsessive involvement in their nerdy young players, but no one before had found it necessary to prevent their publication.

It seems that Steve Jackson had hired the wrong writer. The managing editor of Steve Jackson Games is a former cracker, known by his fellows in the Legion of Doom as The Mentor. At the time of the raid, he and the rest of Jackson staff had been working for over a year on a game called GURPS Cyberpunk, High-Tech Low-Life Role-Playing.

At the time of the Secret Service raids, the game resided entirely on

the hard disks they confiscated. Indeed, it was their target. They told Jackson that, based on its author's background, they had reason to believe it was a "handbook on computer crime." It was therefore inappropriate for publication, 1st Amendment or no 1st Amendment.

I got a copy of the game from the trunk of The Mentor's car in an Austin parking lot. Like the Bell South document, it seemed pretty innocuous to me, if a little inscrutable. Borrowing its flavor from the works of William Gibson and Austin sci-fi author Bruce Sterling, it is filled with silicon brain implants, holodecks, and gauss guns.

It is, as the cover copy puts it, "a fusion of the dystopian visions of George Orwell and Timothy Leary." Actually, without the gizmos, it describes a future kind of like the present its publisher is experiencing at the hands of the Secret Service.

An unbelievably Byzantine world resides within its 120 large pages of small print. (These roll-players must be some kind of idiots savants...) Indeed, it's a thing of such complexity that I can't swear there's no criminal information in there, but then I can't swear that Grateful Dead records don't have satanic messages if played backwards. Anything's possible, especially inside something as remarkable as Cyberpunk.

The most remarkable thing about Cyberpunk is the fact that it was printed at all. After much negotiation, Jackson was able to get the Secret Service to let him have some of his data back. However, they told him that he would be limited to an hour and a half with only one of his three computers. Also, according to Jackson, "They insisted that all the copies be made by a Secret Service agent who was a two-finger typist. So we didn't get much. "

In the end, Jackson and his staff had to reconstruct most of the game from neural rather than magnetic memory. They did have a few very old backups, and they retrieved some scraps which had been passed around to game testers. They also had the determination of the enraged.

Despite government efforts to impose censorship by prior restraint, Cyberpunk is now on the market. Presumably, advertising it as "The book that was seized by the U.S. Secret Service" will invigorate sales. But Steve Jackson Games, the heretofore prosperous publisher of more than a hundred role-playing games, has been forced to lay off more than half of its employees and may well be mortally wounded.

Any employer who has heard this tale will think hard before he hires a computer cracker. Which may be, of course, among the effects the Secret Service desires.

******

On May 8, 1990, Operation Sun Devil, heretofore an apparently random and nameless trickle of Secret Service actions, swept down on the Legion of Doom and its ilk like a bureaucratic tsunami. On that day, the Secret Service served 27 search warrants in 14 cities from Plano, Texas to New York, New York.

The law had come to Cyberspace. When the day was over, transit through the wide open spaces of the Virtual World would be a lot trickier.

In a press release following the sweep, the Secret Service boasted having shut down numerous computer bulletin boards, confiscated 40 computers, and seized 23,000 disks. They noted in their statement that "the conceivable criminal violations of this operation have serious implications for the health and welfare of all individuals, corporations, and United States Government agencies relying on computers and telephones to communicate."

It was unclear from their statement whether "this operation" meant the Legion of Doom or Operation Sun Devil. There was room to interpret it either way.

Because the deliciously ironic truth is that, aside from the 3 page Bell South document, the hackers had neither removed nor damaged anyone's data. Operation Sun Devil, on the other hand, had "serious implications" for a number of folks who relied on "computers and telephones to communicate." They lost the equivalent of about 5.4 million pages of information. Not to mention a few computers and telephones.

And the welfare of the individuals behind those figures was surely in jeopardy. Like the story of the single mother and computer consultant in Baltimore whose sole means of supporting herself and her 18 year old son was stripped away early one morning. Secret Service agents broke down her door with sledge hammers, entered with guns drawn, and seized all her computer equipment. Apparently her son had also been using it...

Or the father in New York who opened the door at 6:00 AM and found a shotgun at his nose. A dozen agents entered. While one of the kept the man's wife in a choke-hold, the rest made ready to shoot and entered the bedroom of their sleeping 14 year-old. Before leaving, they confiscated every piece of electronic equipment in the house, including all the telephones.

It was enough to suggest that the insurance companies should start writing policies against capricious governmental seizure of circuitry.

In fairness, one can imagine the government's problem. This is all pretty magical stuff to them. If I were trying to terminate the operations of a witch coven, I'd probably seize everything in sight. How would I tell the ordinary household brooms from the getaway vehicles?

But as I heard more and more about the vile injustices being heaped on my young pals in the Legion of Doom, not to mention the unfortunate folks nearby, the less I was inclined toward such temperate thoughts as these. I drifted back into a 60's-style sense of the government, thinking it a thing of monolithic and evil efficiency and adopting an up-against-the-wall willingness to spit words like "pig" or "fascist" into my descriptions.

In doing so, I endowed the Secret Service with a clarity of intent which no agency of government will ever possess. Despite almost every experience I've ever had with federal authority, I keep imagining its competence.

For some reason, it was easier to invest the Keystone Kapers of Operation Sun Devil with malign purpose rather than confront their absurdity straight-on. There is, after all, a twisted kind of comfort in political paranoia. It provides one such a sense of orderliness to think that the government is neither crazy nor stupid and that its plots, though wicked, are succinct.

I was about to have an experience which would restore both my natural sense of unreality and my unwillingness to demean the motives of others. I was about to see first hand the disorientation of the law in the featureless vastness of Cyberspace.

****

In Search of NuPrometheus

"I pity the poor immigrant..."
-- Bob Dylan

Sometime last June, an angry hacker got hold of a chunk of the highly secret source code which drives the Apple Macintosh. He then distributed it to a variety of addresses, claiming responsibility for this act of information terrorism in the name of the NuPrometheus League.

Apple freaked. NuPrometheus had stolen, if not the Apple crown jewels, at least a stone from them. Worse, NuPrometheus had then given this prize away. Repeatedly.

All Apple really has to offer the world is the software which lies

encoded in silicon on the ROM chip of every Macintosh. This set of instructions is the cyber-DNA which makes a Macintosh a Macintosh.

Worse, much of the magic in this code was put there by people who not only do not work for Apple any longer, but might only do so again if encouraged with cattle prods. Apple's attitude toward its ROM code is a little like that of a rich kid toward his inheritance. Not actually knowing how to create wealth himself, he guards what he has with hysterical fervor.

Time passed, and I forgot about the incident. But one recent May morning, I leaned that others had not. The tireless search for the spectral heart of NuPrometheus finally reached Pinedale, Wyoming, where I was the object of a two hour interview by Special Agent Richard Baxter, Jr. of the Federal Bureau of Investigation.

Poor Agent Baxter didn't know a ROM chip from a Vise-grip when he arrived, so much of that time was spent trying to educate him on the nature of the thing which had been stolen. Or whether "stolen" was the right term for what had happened to it.

You know things have rather jumped the groove when potential suspects must explain to law enforcers the nature of their alleged perpetrations.

I wouldn't swear Agent Baxter ever got it quite right. After I showed him some actual source code, gave a demonstration of e-mail in action, and downloaded a file from the WELL, he took to rubbing his face with both hands, peering up over his finger tips and saying, "It sure is something, isn't it" Or, "Whooo-ee."

Or "my eight year-old knows more about these things than I do." He didn't say this with a father's pride so much as an immigrant's fear of a strange new land into which he will be forcibly moved and in which his own child is a native. He looked across my keyboard into Cyberspace and didn't like what he saw.

We could have made it harder for one another, but I think we each sensed that the other occupied a world which was as bizarre and nonsensical as it could be. We did our mutual best to suppress immune response at the border.

You'd have thought his world might have been a little more recognizable to me. Not so, it turns out. Because in his world, I found several unfamiliar features, including these:

1. The Hacker's Conference is an underground organization of computer outlaws with likely connections to, and almost certainly sympathy with, the NuPrometheus League. (Or as Agent Baxter

repeatedly put it, the "New Prosthesis League.")

2. John Draper, the affore-mentioned Cap'n Crunch, in addition to being a known member of the Hacker's Conference, is also CEO and president of Autodesk, Inc. This is of particular concern to the FBI because Autodesk has many top-secret contracts with the government to supply Star Wars graphics imaging and "hyperspace" technology. Worse, Draper is thought to have Soviet contacts.

He wasn't making this up. He had lengthy documents from the San Francisco office to prove it. And in which Autodesk's address was certainly correct.

On the other hand, I know John Draper. While, as I say, he may have once distinguished himself as a cracker during the Pleistocene, he is not now, never has been, and never will be CEO of Autodesk. He did work there for awhile last year, but he was let go long before he got in a position to take over.

Nor is Autodesk, in my experience with it, the Star Wars skunk works which Agent Baxter's documents indicated. One could hang out there a long time without ever seeing any gold braid.

Their primary product is something called AutoCAD, by far the most popular computer-aided design software but generally lacking in lethal potential. They do have a small development program in Cyberspace, which is what they call Virtual Reality. (This, I assume is the "hyperspace" to which Agent Baxter's documents referred.)

However, Autodesk had reduced its Cyberspace program to a couple of programmers. I imagined Randy Walser and Carl Tollander toiling away in the dark and lonely service of their country. Didn't work. Then I tried to describe Virtual Reality to Agent Baxter, but that didn't work either. In fact, he tilted. I took several runs at it, but I could tell I was violating our border agreements. These seemed to include a requirement that neither of us try to drag the other across into his conceptual zone.

I fared a little better on the Hacker's Conference. Hardly a conspiracy, the Hacker's Conference is an annual convention originated in 1984 by the Point Foundation and the editors of Whole Earth Review. Each year it invites about a hundred of the most gifted and accomplished of digital creators. Indeed, they are the very people who have conducted the personal computer revolution. Agent Baxter looked at my list of Hacker's Conference attendees and read their bios.

"These are the people who actually design this stuff, aren't they?" He was incredulous. Their corporate addresses didn't fit his model of

outlaws at all well.

Why had he come all the way to Pinedale to investigate a crime he didn't understand which had taken place (sort of) in 5 different places, none of which was within 500 miles?

Well, it seems Apple has told the FBI that they can expect little cooperation from Hackers in and around the Silicon Valley, owing to virulent anti-Apple sentiment there. They claim this is due to the Hacker belief that software should be free combined with festering resentment of Apple's commercial success. They advised the FBI to question only those Hackers who were as far as possible from the twisted heart of the subculture.

They did have their eye on some local people though. These included a couple of former Apple employees, Grady Ward and Water Horat, Chuck Farnham (who has made a living out of harassing Apple), Glenn Tenney (the purported leader of the Hackers), and, of course, the purported CEO of Autodesk.

Other folks Agent Baxter asked me about included Mitch Kapor, who wrote Lotus 1-2-3 and was known to have received some this mysterious source code. Or whatever. But I had also met Mitch Kapor, both on the WELL and in person. A less likely computer terrorist would be hard to come by.

Actually, the question of the source code was another area where worlds but shadow-boxed. Although Agent Baxter didn't know source code from Tuesday, he did know that Apple Computer had told his agency that what had been stolen and disseminated was the complete recipe for a Macintosh computer. The distribution of this secret formula might result in the creation of millions of Macintoshes not made by Apple. And, of course, the ruination of Apple Computer.

In my world, NuPrometheus (whoever they, or more likely, he might be) had distributed a small portion of the code which related specifically to Color QuickDraw. QuickDraw is Apple's name for the software which controls the Mac's on-screen graphics. But this was another detail which Agent Baxter could not capture. For all he knew, you could grow Macintoshes from floppy disks.

I explained to him that Apple was alleging something like the ability to assemble an entire human being from the recipe for a foot, but even he know the analogy was inexact. And trying to get him to accept the idea that a corporation could go mad with suspicion was quite futile. He had a far different perception of the emotional reliability of institutions.

When he fnally left, we were both dazzled and disturbed. I spent some time thinking about Lewis Carroll and tried to return to writing about the legal persecution of the Legion of Doom. But my heart wasn't in it. I found myself suddenly too much in sympathy with Agent Baxter and his struggling colleagues from Operation Sun Devil to get back into a proper sort of pig-bashing mode.

Given what had happened to other innocent bystanders like Steve Jackson, I gave some thought to getting scared. But this was Kafka in a clown suit. It wasn't precisely frightening. I also took some comfort in a phrase once applied to the administration of Frederick the Great: "Despotism tempered by incompetence."

Of course, incompetence is a double-edged banana. While we may know this new territory better than the authorities, they have us literally out-gunned. One should pause before making well-armed paranoids feel foolish, no matter how foolish they seem.

******

The Fear of White Noise

"Neurosis is the inability to tolerate ambiguity."

-- Sigmund Freud, appearing to me in a dream

I'm a member of that half of the human race which is inclined to divide the human race into two kinds of people. My dividing line runs between the people who crave certainty and the people who trust chance.

You can draw this one a number of ways, of course, like Control vs. Serendipity, Order vs. Chaos, Hard answers vs. Silly questions, or Newton, Descartes & Aquinas vs. Heisenberg, Mandelbrot & the Dalai Lama. Etc.

Large organizations and their drones huddle on one end of my scale, busily trying to impose predictable homogeneity on messy circumstance. On the other end, free-lancers and ne'er-do-wells cavort about, getting by on luck if they get by at all.

However you cast these poles, it comes down to the difference between those who see life as a struggle against cosmic peril and human infamy and those who believe, without any hard evidence, that the universe is actually on our side. Fear vs. Faith.

I am of the latter group. Along with Gandhi and Rebecca of Sunnybrook Farm, I believe that other human beings will quite

consistently merit my trust if I'm not doing something which scares them or makes them feel bad about themselves. In other words, the best defense is a good way to get hurt.

In spite of the fact that this system works very reliably for me and my kind, I find we are increasingly in the minority. More and more of our neighbors live in armed compounds. Alarms blare continuously. Potentially happy people give their lives over to the corporate state as though the world were so dangerous outside its veil of collective immunity that they have no choice.

I have a number of theories as to why this is happening. One has to do with the opening of Cyberspace. As a result of this development, humanity is now undergoing the most profound transformation of its history. Coming into the Virtual World, we inhabit Information. Indeed, we become Information. Thought is embodied and the Flesh is made Word. It's weird as hell.

Beginning with the invention of the telegraph and extending through television into Virtual Reality, we have been, for a over a century, experiencing a terrifying erosion in our sense of both body and place. As we begin to realize the enormity of what is happening to us, all but the most courageous have gotten scared.

And everyone, regardless of his psychic resilience, feels this overwhelming sense of strangeness. The world, once so certain and tangible and legally precise, has become an infinite layering of opinions, perceptions, litigation, camera-angles, data, white noise, and, most of all, ambiguities. Those of us who are of the fearful persuasion do not like ambiguities.

Indeed, if one were a little jumpy to start with, he may now be fairly humming with nameless dread. Since no one likes his dread to be nameless, the first order of business is to find it some names.

For a long time here in the United States, Communism provided a kind of catch-all bogeyman. Marx, Stalin and Mao summoned forth such a spectre that, to many Americans, annihilation of all life was preferable to the human portion's becoming Communist. But as Big Red wizened and lost his teeth, we began to cast about for a replacement.

Finding none of sufficient individual horror, we have draped a number of objects with the old black bunting which once shrouded the Kremlin. Our current spooks are terrorists, child abductors, AIDS, and the underclass. I would say drugs, but anyone who thinks that the War on Drugs is not actually the War on the Underclass hasn't been paying close enough attention.

There are a couple of problems with these Four Horsemen. For one thing, they aren't actually very dangerous. For example, only 7 Americans died in worldwide terrorist attacks in 1987. Fewer than 10 (out of about 70 million) children are abducted by strangers in the U.S. each year. Your chances of getting AIDS if you are neither gay nor a hemophiliac nor a junkie are considerably less than your chances of getting killed by lightning while golfing. The underclass is dangerous, of course, but only, with very few exceptions, if you are a member of it.

The other problem with these perils is that they are all physical. If we are entering into a world in which no one has a body, physical threats begin to lose their sting.

And now I come to the point of this screed: The perfect bogeyman for Modern Times is the Cyberpunk! He is so smart he makes you feel even more stupid than you usually do. He knows this complex country in which you're perpetually lost. He understands the value of things you can't conceptualize long enough to cash in on. He is the one-eyed man in the Country of the Blind.

In a world where you and your wealth consist of nothing but beeps and boops of micro-voltage, he can steal all your assets in nanoseconds and then make you disappear.

He can even reach back out of his haunted mists and kill you physically. Among the justifications for Operation Sun Devil was this chilling tidbit:

"Hackers had the ability to access and review the files of hospital patients.
Furthermore, they could have added, deleted, or altered vital patient information, possibly causing life- threatening situations."

Perhaps the most frightening thing about the Cyberpunk is the danger he presents to The Institution, whether corporate or governmental. If you are frightened you have almost certainly taken shelter by now in one of these collective organisms, so the very last thing you want is something which can endanger your heretofore unassailable hive.

And make no mistake, crackers will become to bureaucratic bodies what viruses presently are to human bodies. Thus, Operation Sun Devil can be seen as the first of many waves of organizational immune response to this new antigen. Agent Baxter was a T-cell. Fortunately, he didn't know that himself and I was very careful not to show him my own antigenic tendencies.

I think that herein lies the way out of what might otherwise become an Armageddon between the control freaks and the neo-hip. Those who are comfortable with these disorienting changes must do everything in our power to convey that comfort to others. In other words, we must share our sense of hope and opportunity with those who feel that in Cyberspace they will be obsolete eunuchs for sure.

It's a tall order. But, my silicon brothers, our self-interest is strong. If we come on as witches, they will burn us. If we volunteer to guide them gently into its new lands, the Virtual World might be a more amiable place for all of us than this one has been.

Of course, we may also have to fight.

******

Defining the conceptual and legal map of Cyberspace before the ambiguophobes do it for us (with punitive over-precision) is going to require some effort. We can't expect the Constitution to take care of itself. Indeed, the precedent for mitigating the Constitutional protection of a new medium has already been established. Consider what happened to radio in the early part of this century.

Under the pretext of allocating limited bandwidth, the government established an early right of censorship over broadcast content which still seems directly unconstitutional to me. Except that it stuck. And now, owing to a large body of case law, looks to go on sticking.

New media, like any chaotic system, are highly sensitive to initial conditions. Today's heuristical answers of the moment become tomorrow's permanent institutions of both law and expectation. Thus, they bear examination with that destiny in mind.

Earlier in this article, I asked a number of tough questions relating to the nature of property, privacy, and speech in the digital domain. Questions like: "What are data and what is free speech?" or "How does one treat property which has no physical form and can be infinitely reproduced?" or "Is a computer the same as a printing press." The events of Operation Sun Devil were nothing less than an effort to provide answers to these questions. Answers which would greatly enhance governmental ability to silence the future's opinionated nerds.

In over-reaching as extravagantly as they did, the Secret Service may actually have done a service for those of us who love liberty. They have provided us with a devil. And devils, among their other galvanizing virtues, are just great for clarifying the issues and putting

iron in your spine. In the presence of a devil, it's always easier to figure out where you stand.

While I previously had felt no stake in the obscure conundra of free telecommunication, I was, thanks to Operation Sun Devil, suddenly able to plot a trajectory from the current plight of the Legion of Doom to an eventual constraint on opinions much dearer to me. I remembered Martin Neimoeller, who said:

"In Germany they came first for the Communists, and I didn't speak up because I wasn't a Communist. Then they came for the Jews, and I didn't speak up because I wasn't a Jew. They came for the trade unionists, and I didn't speak up because I wasn't a trade unionist. Then they came for the Catholics, and I didn't speak up because I was a Protestant. Then they came for me, and by that time no one was left to speak up."

I decided it was time for me to speak up.

The evening of my visit from Agent Baxter, I wrote an account of it which I placed on the WELL. Several days later, Mitch Kapor literally dropped by for a chat.

Also a WELL denizen, he had read about Agent Baxter and had begun to meditate on the inappropriateness of leaving our civil liberties to be defined by the technologically benighted. A man who places great emphasis on face-to-face contact, he wanted to discuss this issue with me in person. He had been flying his Canadair bizjet to a meeting in California when he realized his route took him directly over Pinedale.

We talked for a couple of hours in my office while a spring snowstorm swirled outside. When I recounted for him what I had learned about Operation Sun Devil, he decided it was time for him to speak up too.

He called a few days later with the phone number of a civil libertarian named Harvey Silverglate, who, as evidence of his conviction that everyone deserves due process, is currently defending Leona Helmsley. Mitch asked me to tell Harvey what I knew, with the inference that he would help support the costs which are liable to arise whenever you tell a lawyer anything.

I found Harvey in New York at the offices of that city's most distinguished constitutional law firm, Rabinowitz, Boudin, Standard, Krinsky, and Lieberman. These are the folks who made it possible for the New York Times to print the Pentagon Papers. (Not to dwell on the unwilling notoriety which partner Leonard Boudin achieved back in 1970 when his Weathergirl daughter blew up the family home...)

In the conference call which followed, I could almost hear the skeletal click as their jaws dropped. The next day, Eric Lieberman and Terry Gross of Rabinowitz, Boudin met with Acid Phreak, Phiber Optik, and Scorpion.

The maddening trouble with writing this account is that Whole Earth Review, unlike, say, Phrack, doesn't publish instantaneously. Events are boiling up at such a frothy pace that anything I say about current occurrences surely will not obtain by the time you read this. The road from here is certain to fork many times. The printed version of this will seem downright quaint before it's dry.

But as of today (in early June of 1990), Mitch and I are legally constituting the Electronic Frontier Foundation, a two (or possibly three) man organization which will raise and disburse funds for education, lobbying, and litigation in the areas relating to digital speech and the extension of the Constitution into Cyberspace.

Already, on the strength of preliminary stories about our efforts in the Washington Post and the New York Times, Mitch has received an offer from Steve Wozniak to match whatever funds he dedicates to this effort. (As well as a fair amount of abuse from the more institutionalized precincts of the computer industry.)

The Electronic Frontier Foundation will fund, conduct, and support legal efforts to demonstrate that the Secret Service has exercised prior restraint on publications, limited free speech, conducted improper seizure of equipment and data, used undue force, and generally conducted itself in a fashion which is arbitrary, oppressive, and unconstitutional.

In addition, we will work with the Computer Professionals for Social Responsibility and other organizations to convey to both the public and the policy-makers metaphors which will illuminate the more general stake in liberating Cyberspace.

Not everyone will agree. Crackers are, after all, generally beyond public sympathy. Actions on their behalf are not going to be popular no matter who else might benefit from them in the long run.

Nevertheless, in the litigations and political debates which are certain to follow, we will endeavor to assure that their electronic speech is protected as certainly as any opinions which are printed or, for that matter, screamed. We will make an effort to clarify issues surrounding the distribution of intellectual property. And we will help to create for America a future which is as blessed by the Bill of Rights as its past has been.

John Perry Barlow barlow@well.sf.ca.us Friday, June 8, 1990

CYBERLAW REPORT ON THE SJ GAMES CASE

CyberLaw is an educational service focusing on legal issues concerning computer technology. CyberLex reports legal developments touching the computer industry. CyberLaw and CyberLex are distributed as a monthly column, published by computer user groups throughout the United States.

CyberLaw is edited by Jonathan Rosenoer (jrsnr@well.sf.ca.us)

CyberLaw (tm) [4/93]

Search & Seizure

I. Liberty & Cyberspace

Three years ago, a small publisher of role-playing games in Texas was raided by the United States Secret Service. Government agents carted away computers, one of which ran the company's computer bulletin board system (BBS), hundreds of floppy disks, and drafts of a soon-to-be-published book and of magazine articles. The seized material was held for months, which led to the layoff of a number of the company's employees. No-one at the company was arrested or charged with a crime. The owner of the company, Steve Jackson, appealed for help and managed to gain the attention of some prominent members of the computer community. The case came to be viewed by many as a struggle for civil liberties in the new electronic frontier, known as Cyberspace. Steve Jackson and his supporters were vindicated recently, when a Federal District Court ruled that the Secret Service had violated federal statutes protecting publishers and the privacy of electronic communications with regard to its raid of the company.

II. The Saga Begins

The saga of Steve Jackson and his company began in the summer of 1989, when the Secret Service was contacted by a representative of BellSouth (a Regional Bell Operating Company) who advised that there had been a theft of sensitive data from BellSouth's computer system. The stolen data was described as "an internal, proprietary document that described the control, operation and maintenance of BellSouth's 911 emergency system." This report led the Secret Service and the U.S. Attorney's office in Chicago into a larger

investigation, concerning a national group of computer hackers called the "Legion of Doom" (LOD).

A member of LOD had allegedly entered a BellSouth computer and copied the 911 document to his own computer. The 911 document was then allegedly sent to a BBS in Illinois, from which it was downloaded by a student named Craig Neidorf and edited for and distributed in a publication named __Phrack__. One person who received __Phrack__ was Loyd Blankenship, also a member of LOD.

Notably, the 911 document is not a computer program and has nothing to do with accessing a 911 system. It simply details who does what in the telephone company bureaucracy regarding customer complaints and equipment failures, among other things. For the Secret Service, BellSouth estimated the cost of the 911 document at $79,449. But in July 1990, during Neidorf's trial, it was disclosed that the 911 document was available to the public directly from BellSouth for about $20. (Upon this disclosure, the prosecution of Neidorf collapsed -- leaving him owing over $100,000 in legal fees.)

In early 1990, the Secret Service learned that another LOD member had posted a message on a BBS maintained by Blankenship, allegedly "inviting other BBS participants to send in encrypted passwords stolen from other computers, which Blankenship and [the other member of LOD] would decrypt and return...." After seeking additional information, the Secret Service decided to obtain search warrants to obtain evidence against them, including a search warrant for the offices of Blankenship's employer, Steve Jackson Games, Inc.

Steve Jackson Games, as described by its lawyers, "publishes role-playing games in book form, magazines, a book about game theory, boxed games, and game-related products. The company's games are played not on computers, but with dice, a game book or books, and lots of imagination." As part of its business, the company runs a BBS (the "Illuminati" BBS) that allows outside callers to dial in and, as outlined by Steve Jackson, "read messages left by [the company], read public messages left by others who have called the bulletin board, leave public messages for other callers to read, send private electronic mail to other persons who called the bulletin board, and 'download' computerized files to their own computer." Like the typical BBS, the Illuminati BBS stored electronic mail, including mail that had been sent but not yet received. In February 1990, there were 365 users of the Illuminati BBS and, according to the trial court, Blankenship was a "co-sysop" of the BBS.

III. The Raid

On March 1, 1990, Steve Jackson Games was raided by the Secret Service. They seized and carried away a computer found on Blankenship's desk, a disassembled computer next to his desk, the computer running the Illuminati BBS, over 300 computer disks, and various documents and other materials. Among the seized items were drafts of a book titled __GURPS Cyberpunk__, which was to be published within days or weeks of the raid, and drafts of magazines and magazine articles. ("GURPS" stands for "Generic Universal Game Role Playing System.") According to the company's attorneys, a Secret Service agent called __GURPS Cyberpunk__ "'a handbook for computer crime' in Mr. Jackson's presence, (although the government now claims that the book was not the target of the search and admits it was not evidence of any crime)."

For Steve Jackson Games, the raid was a calamity. It was suffering severe cash flow problems, and the seizure caused substantial delays in publication and the termination of 8 employees. The bulk of the seized material was not made available to the company until late June 1990, and no printed copies of __GURPS Cyberpunk__ were ever returned.

The raid also caused wide concern across the United States. From the outset, as noted by the company's lawyers, many saw the case as one in which,

"The Secret Service, on exceedingly weak pretense, invaded the office of an upstanding, hard-working small businessman, and nearly put him out of business. The Secret Service shut down a working BBS -- a new, powerful means of public and private communication -- with __no__ evidence that anything unlawful was transpiring there. Shutting down the "Illuminati" was like clearing or closing down a park or meeting hall, simply because one of hundreds of the people gathered there was under vague suspicion."

This view was later validated by the trial court, which found that,

"[P]rior to March 1, 1990, and at all other times, __there has never been any basis for suspicion__ that [Steve Jackson Games, Steve Jackson, or any of the other individuals who subsequently sued the Secret Service as a result of the raid] have engaged in any criminal activity, violated any law, or attempted to communicate, publish, or store any illegally obtained information or otherwise provide access

to any illegally obtained information or to solicit any information which was to be used illegally." (Emphasis added.)

IV. The Lawsuit

After the raid, Steve Jackson Games, Steve Jackson and 3 users of the Illuminati BBS filed suit against the United States Secret Service, the United States of America, and several government employees who had been involved in the raid. The plaintiffs brought causes of action for violation of the following: the Fourth Amendment to the U.S. Constitution; the Privacy Protection Act, 42 U.S.C. 2000aa et seq.; the Wire and Electronic Communications Interception and Interception of Oral Communication Act, 18 U.S.C. 2510 et seq.; and, the Stored Wire and Electronic Communications and Transactional Records Act, 18 U.S.C. 2701 et seq. (The latter 2 statutes are part of the Electronic Communications Protection Act, or ECPA.)

V. Fourth Amendment

With respect to the Fourth Amendment, the plaintiffs argued that "probable cause to believe that a crime has occurred ... does not automatically give license to search every place that a suspect may frequent," and also that "there must be probable cause to believe that the __type__ of materials sought are located at the place to be searched." "The search warrant," continued the plaintiffs, "did not establish probable cause that evidence of any crime would be found at [Steve Jackson Games]," and the search of the company "was broader than justified by any facts in the warrant." In response, the government argued that even if the plaintiffs were correct, they still had to prove that "these defects were so obvious that no reasonable officer could have believed the warrant to be valid, in light of the information [the officer] possessed." Because a court determination in favor of the plaintiffs could have resulted in an immediate appeal that would delay the balance of their case, the plaintiffs dropped their Fourth Amendment claims to focus their case on the Privacy Protection Act and ECPA claims.

VI. Privacy Protection Act

The Privacy Protection Act concerns the investigation and prosecution of criminal offenses and, in relevant part, prohibits government employees from searching for or seizing any "work product materials" possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication. "Work

product materials" are defined to include materials, not including contraband, the fruits of a crime, or things used as the means of committing a crime, created or prepared for the purpose of communicating such materials to the public.

At the time of the raid on Steve Jackson Games, the Secret Service was advised that the company was in the publishing business. No significance was attached to this information, however, as the Secret Service agents involved in the raid were oblivious of the provisions of the Privacy Protection Act.

Notwithstanding the fact that the Secret Service had failed to make a reasonable investigation of Steve Jackson Games "when it was apparent [its] intention was to take substantial properties belonging to the [company], the removal of which could have a substantial effect on the continuation of business," the trial court declined to find
that on March 1, 1990, any government employee had reason to believe that the property to be seized would be "work product material" subject to the Privacy Protection Act. But during the raid, the Secret Service had been advised of facts that put its agents on notice of probable violations of that Act. Indeed, the Secret Service continued to detain the company's property through late June 1990 despite the fact that, as observed by the trial court, "[i]mmediate arrangements could and should have been made on March 2, 1990, whereby copies of all information seized could have been made." The refusal of the Secret Service to return the company's information and property violated the Privacy Protection Act, and the court awarded Steve Jackson Games its expenses ($8,781) and economic damages ($42,259).

VII. ECPA

The trial court did not find, however, that the Secret Service had violated the Electronic Communications Interception and Interception of Oral Communication Act. According to the trial court, "the Secret Service intended not only to seize and read [the communications stored on the Illuminati BBS], but, in fact, did read the communications and thereafter deleted or destroyed some communications either intentionally or accidentally." But the Secret Service had not "intercepted" communications within the meaning of the latter Act, ruled the court, apparently on the grounds that only the contemporaneous acquisition of a communication is prohibited thereby.

In support of this ruling, the court looked to the Congressional enactment of the Stored Wire and Electronic Communications and Transactional Records Act, among other things. This statute protects the content of electronic communications in electronic storage and sets out specific requirements for the government to follow to obtain the "disclosure" of such communications. One such requirement is that there be "reason to believe the contents of a[n] ... electronic communication ... are relevant to a legitimate law enforcement inquiry." Although the Secret Service wanted to seize, review and read all electronic communications, public and private, on the Illuminati BBS, the Secret Service did not advise the Magistrate Judge who issued the warrant for the raid on Steve Jackson Games "that the Illuminati board contained private electronic communications between users or how the disclosure of the content of these communications could relate to [the] investigation." The court commented that it was not until June 1990 that the plaintiffs were able to determine the reasons for the March 1, 11990, seizure, "and then only with the efforts of the offices of both United States Senators of the State of Texas." Simply stated, "[t]he procedures followed by the Secret Service in this case virtually eliminated the safeguards contained in the statute." Lacking sufficient proof of compensatory damages, the court assessed statutory damages in favor of the plaintiffs, in the amount of $1,000 for each plaintiff.

VIII. Further Information

Further information concerning this case may be found in the opinion of the United States District Court in __Steve Jackson Games, Inc., et al. v. United States Secret Service, et al.__, No. A-91-CA-346-SS (W.D. Tex. 3/12/93). For background information on this case and other related cases, see B. Sterling, __The Hacker Crackdown__ (1992), and John Perry Barlow, __Crime & Puzzlement__ (1990).

(Copies of the arguments filed with the trial court and of the court's opinion were kindly made available to the author by Peter D. Kennedy, Esq., of George, Donaldson & Ford, attorneys for Steve Jackson Games, Inc. and the other plaintiffs.)

Notable legal developments reported in April 1993 include the following:

#The Ninth Circuit Court of Appeals has ruled that an independent service provider violated copyright laws by loading operating software licensed to its client into the random access memory of its client's computer in the course of fixing the computer. (__MAI Systems Corp. v. Peak Computer Inc., et al.__, 93 C.D.O.S. 2596 (9th Cir. 4/9/93)).

#The White House has announced the development of a computer chip, called the "Clipper Chip," that encodes voice and data transmissions using a secret algorithm. The chip is to work with an 80-bit, split key escrow system. Two escrow agents would each hold 40-bit segments of a user's key, which would be released to law enforcement agents upon presentation of a valid warrant. After the announcement, several groups expressed concern that, among other things, the algorithm used cannot be trusted unless it is public and open to testing. (New York Times, April 16, 1993, A1; San Jose Mercury News, April 16, 1993, 1A, and April 17, 1993, 11D;Wall Street Journal, April 19, 1993, A5.)

#The CIA has warned U.S. high-tech companies that the French government may be spying on them. (San Jose Mercury News, April 27, 1993, 11E.)

#Kevin Poulson, a hacker already scheduled to be tried on 14 federal felonies, has been indicted on 19 more felony counts in which he is accused of using telephone and computer skills to ensure that he and two alleged accomplices would win radio station call-in contests. Prizes in those contest included a pair of Porsche cars and more than $20,00 in cash. (San Jose Mercury News, April 22, 1993, 1F.)

#InterDigital Communications Corp. has filed suit for patent infringement against Oki Electric Industry Co., of Tokyo. The suit concerns a data communication technique called code division multiple access (CDMA), developed by a San Diego-based company, and CDMA-based phones that Oki plans to manufacture, among other things. InterDigital holds many patents on a rival technique called time division multiple access, used by several cellular phone companies. (Wall Street Journal, April 19, 1993, 7B.)

#20 Japanese telecommunications companies announced that

they will join Motorola's Iridium project, a planned digital cellular telephone network linked by 66 orbiting satellites. (San Jose Mercury News, April 3, 1993, 11D.)

#The nation's local phone companies offered to build the "information superhighway" promoted by Vice President Al Gore if they are allowed to go back onto the long-distance phone business, to manufacture equipment, and to provide video programming over phone lines. (San Jose Mercury News, April 16, 1993, 3C.)

#Apple Computer, Inc. is fighting a $290 million claim by the IRS for back taxes for the years 1987 and 1988 relating to the value of property transferred between foreign and domestic units of the company. (San Jose Mercury News, April 3, 1993, 9D.)

#A federal judge overturned a jury verdict that AMD did not have the right to use Intel microcode in AMD chips, and granted a new trial. The basis for the court's ruling was that Intel had failed to
produce critical documents that would have allowed AMD fairly to present its defense. The verdict had stopped AMD from selling a clone of Intel's 486 microprocessor. Within 2 weeks, Intel sued AMD alleging that AMD's 486 clones and an AMD chip not yet on the market violate Intel copyrights. (San Jose Mercury News, April 17, 1993, 1A, and April 29, 1993, 1C; New York Times, April 17, 1993, p.17.)

#The Commerce Department has imposed permanent import duties of up to 11.45% on Korean-made computer memory chips, following an International Trade Commission finding of "dumping" by South Korean manufacturers. (San Jose Mercury News, April 23, 1993, 1C.)

#Taiwan has adopted a set of copyright law revisions. (San Jose Mercury News, April 23, 1993, 3C.)

#The International Trade Commission has agreed to investigate claims by a Mississippi inventor that 20 computer disk-drive manufacturers are violating a patent he holds for placing carbon coating on computer disks by importing drives that use the technology. One manufacturer, Connor Peripherals Inc., has filed suit to declare the inventor's patent invalid. (San Jose Mercury News, April 27, 1993, 9E.)

Steve Jackson Games | SJ Games vs. the Secret Service

Practical Privacy Protection, Unless Congress Prohibits It

by Jim Warren

This column concerns our futures that we can create, *if* we protect our options.

Protecting Against Peepers

Computer and electronic-mail users are becoming increasingly concerned about information pirates and email eavesdroppers.

Some naive folks think legislation will halt such intrusion.

Realists, however, are urging technical protections against technological surveillance. Numerous speakers at the Computers, Freedom & Privacy Conference stated that the *only* real protection against such surveillance and data theft is robust, verifiably-secure encryption.

Many say "public key" crypto is the most secure--and also the most easily used. It's actually a two-key system, a "key" being simply a number. Everyone can have your "public" key, using it to encrypt information for you. But only you, knowing the "private" half of your two-part key, can decrypt the data.

Recently, numerous major companies have joined, or appear about to join, the public-key bandwagon. They include DEC, Sun, Apple, Microsoft, Lotus, Novell, etc.. They seem likely to endorse the public-key implementation developed by RSA Data Security (Redwood City).

Locksmiths Need Agreement

In all cases, the transmitter must have an encryption tool--a program or device, and the receiver must have a matching decryption tool. Thus, there must be widespread agreement on any crypto that is to be widely used.

The US government adopted the Data Encryption Standard (DES). But its 56-bit key was publicly proven crackable by Stanford's Marty Hellman, even before DES was adopted. The National Security Agency (NSA) opposed Marty's recommendation of an uncrackable 64-bit key.

Further, there are widespread--unproven--rumors that NSA has a "back door" into anything encrypted with DES, so they don't even need a Cray to crack it. Its source code was never released by IBM and NSA, its developers, so users cannot verify that it's secure.

Protecting Fax & Phone

On related fronts, the SecureFX fax encryptor can protect fax transmissions (from Cylink, Sunnyvale). It reportedly includes RSA-licensed public-key crypto, has tamper detection that zeroes-out keys before they can be read, and works with any pair of standard faxes. Each fax plugs into a SecureFX, plugged into the phone line. Sadly, the units cost about four times what a fax costs. (Watch for faxes with built-in crypto.)

Fujitsu may be the first offering a cordless consumer telephone that scrambles communication between the handset and the base-station (Azet-R10). This will render most nosy neighbors' scanners useless and force wire-tappers back onto the telephone poles.

Who's Peeping?

On the other hand, undetectable monitoring of any voice, fax or data phond-line--from anywhere in the nation--is reportedly implemented in current-generation US phone systems. These optional surveillance facilities are reportedly far beyond anything the telcos ever requested or showed any interest in wanting.

Even more curious: Local and state police have said *they* can't get use of it, even for a court-authorized phone tap. They still have to climb a pole or clip onto lines in the central office (c.o.), just like J. Edgar Hoover's surveillance of the Kennedys, Martin Luther King and '60s pacifist groups. [pacifist: someone who's always trying to start a peace]

So--who uses the phone-tap-from-anywhere facilities that the telcos never wanted and aren't available to local and state cops?

Most Peepers Aren't Crackers

Irresponsible news media and mythological movies have inflamed widespread fear that droves of omnipotent computer crackers will invade every computer--and probably make your microwave irradiate your children, too. Even columnist Jack Anderson's staff got suckered into naively touting cracker terror.

In fact, almost all computer criminals and data-peepers are employees, managers, agents and politicians--working on the inside--using authorized access for covert and/or unauthorized purposes.

Example: The Mayor of Colorado Springs secretly monitored confidential electronic correspondence between members of his City Council, using his access as system operator. (He is also President of the US Council of Mayors.)

Of course, robust, verifiably-secure crypto would cure such automated surveillance. If permitted.

Congressional Call for Guaranteed Insecurity

Early this year, Senators Biden (D-DE) and DeConcini (D-AZ) buried

this sentence in Senate Bill 266, an "omnibus anti-terrorism bill"--introduced on the House side by Rep. Tom Lantos (D-CA):

[A "... providers of electronic communications services and manufacturers of electronic communications service equipment shall *ensure that communications systems permit the government to obtain the plain text contents of voice, data, and other communications* when appropriately authorized by law." [emphasis added]

If this is passed, all US crypto systems will have a hole in them--a back door for "authorized" agents. Industrial and foreign spies wouldn't have to *wonder* whether encrypted data and communications were crackable; the law will guarantee it. Spies would need only to crack it, or simply obtain access through any "authorized agent" they could bribe or blackmail.

Well, Desert Storm died and the terrorist terror went away. (Terrorists are *so* undependable.)

So, this "data insecurity guarantee" promptly resurfaced in an "omnibus anti-crime bill," S618. (US criminals are more reliable than terrorists.)

What's More Important--People or Prosecution?

Admittedly, if secure encryption were available to citizens and companies, criminals might also use it. But, even if law-abiding citizens are prohibited from having secure crypto tools, criminals can still have them--the techniques are widely published and well understood in international computer circles.

Should everybody be permitted to adequately protect their communications and records--or should such security be available only to lawbreakers? Do police and prosecutor needs justify guaranteeing insecurity for everyone else?

The Beltway bureaucrats who insistently push this legislation will only be stopped by a widespread outcry from an informed, vocal public.

Computers, Freedom & Privacy Talks and Tapes Now Available

In the last several months, I've given a number of lectures deriving from this Spring's premier Computers, Freedom & Privacy Conference. And, I gotta say, it is the most exciting and provocative subject I've presented, since '70s lectures about "personal computing"--when microcomputing was an infant industry unknown to an unsuspecting population.

Also, audiotapes of the CFP Conference are (finally!) available. Contact Recording, Etc., Palo Alto CA; (415)327-9344, 321-9261/fax. Pre-tax prices are $14.95/tape, $34.95/day (5 tapes), $59.95/full set (15 tapes).

Contribute Your Two Sense [sic]!

Share *your* fantasies seeking realization. Send 'em to Jim Warren, Realizable Fantasies, 345 Swett Road, Woodside CA 94062. Published

proposals will be attributed to their authors unless anonymity is requested.

Press Releases issued at end of SJ Games v. Secret Service

PRESS RELEASE March 15, 1993 - For Immediate Release

STEVE JACKSON GAMES WINS SUIT AGAINST SECRET SERVICE

Steve Jackson Games and its co-plaintiffs - Steve Jackson himself and three users of the Illuminati Bulletin Board - have won their lawsuit against the US Secret Service. The decision was announced late Friday, March 12.

Federal judge Sam Sparks ruled for SJ Games on the PPA (Privacy Protection Act), saying that the publisher's work product was unlawfully seized and held. Under the ECPA (Electronic Communications Privacy Act), he ruled that the Secret Service had unlawfully read, disclosed and erased the messages - despite their repeated denials that they had done any such thing. On a separate ECPA count, he ruled for the defendants, saying that taking the computer out the door was not an "interception" of the messages on it within the meaning of the law.

The Electronic Frontier Foundation, which sponsored the suit, hailed the decision as "groundbreaking." According to Mike Godwin, legal services counsel for the EFF, "This case should send a message to law-enforcement groups everywhere that they can't ignore the rights of those who communicate by computer."

The judge awarded damages of $1,000 per plaintiff under the ECPA, for a total of $5,000. Under the PPA, he awarded SJ Games $42,259 for lost profits in 1990, and out-of-pocket costs of $8,781. The plaintiff's attorneys are also entitled to costs, an amount which will be well in excess of $200,000.

The Justice Department has not stated whether it will appeal.

Sparks' opinion was quite critical of the Secret Service's behavior, before, during and after their raid, calling the affidavit and warrant preparation "simply sloppy and not carefully done."

Commented Steve Jackson: "I'm overjoyed, and a little numb. We stood up to them and we won. It was never a sure thing . . . legally, this is all new ground. We won because what the Secret Service did to us was totally outrageous, and because our lawyers did a great job of penetrating their cover-up and bringing out all the facts.

"I'm more grateful than I can say to the Electronic Frontier Foundation for making the suit possible. And since the government will have to pay our legal costs, the EFF will get their money back, to fight the next case!

"And if I've gained any notoriety from all this mess, I want to use it to work for changes in the law, to stop this kind of abuse forever."

The EFF press release:

NEWSFLASH! STEVE JACKSON GAMES WINS LAWSUIT AGAINST U. S. SECRET SERVICE

A games publisher has won a lawsuit against the U.S. Secret Service and the federal government in a groundbreaking case involving computer publications and electronic-mail privacy.

In a decision announced Friday, March 12, Judge Sparks of the federal district court for the Western District of Texas announced that the case of Steve Jackson Games et al. versus the U.S. Secret Service and the United States Government has been decided for the plaintiffs.

Judge Sparks awarded more than $50,000 in damages to the plaintiffs, citing lost profits for Steve Jackson Games, violations of the Electronic Communications Privacy Act, and violations of the Privacy Protection Act of 1980. The judge also stated that plaintiffs would be reimbursed for their attorneys' fees.

The judge did not find that Secret Service agents had "intercepted" the electronic communications that were captured when agents seized the Illuminati BBS in an early-morning raid in spring of 1990 as part of a computer-crime investigation. The judge did find, however, that the ECPA had been violated by the agents' seizure of stored electronic communications on the system.

Judge Sparks also found that the Secret Service had violated Steve Jackson Games's rights as a publisher under the Privacy Protection Act of 1980, a federal law designed to limit the ability of law-enforcement agents to engage in searches and seizures of publishers.

Mike Godwin, legal services counsel for the Electronic Frontier Foundation, which has underwritten and supported the case since it was filed in 1991, said he is pleased with the decision. "This case is a major step forward in protecting the rights of those who use computers to send private mail to each other or who use computers to create and disseminate publications."

"Judge Sparks has made it eminently clear that the Secret Service acted irresponsibly," Godwin said. "This case should send a message to law-enforcement groups everywhere that they can't ignore the rights of those who communicate by computer."

Press can contact Mike Godwin at 617-576-4510, or by
pager at 1-800-SKYPAGE, 595-0535.

Steve Jackson Games v. US Secret Service

The Case and its Outcome

by Peter D. Kennedy

George, Donaldson & Ford, 114 W. 7th Street, Suite 100
Austin, Texas 78701
512-495-1400 - Fax: 512-499-0094 - E-mail: gdf.well.sf.ca.us

(The print version of this article appeared in BOARDWATCH Magazine in the July 1993 issue.)

On March 12, 1993, a federal judge in Austin, Texas decided that the US Secret Service broke the law when it searched Steve Jackson Games Inc., and seized its bulletin board system and other computer equipment. The decision in this case has been long-awaited in the computer world, and most observers have hailed it as a significant victory for computer user's freedom and privacy.

I had the fortune to be one of the lawyers representing Steve Jackson and his co-plaintiffs. During the course of the lawsuit, I met many people passionately interested in the issues the case raised. I watched and listened to the discussions and arguments about the case. I've been impressed by the intelligence of the on-line world, and the interest that computer enthusiasts show -- especially computer communication enthusiasts -- in the law. I've also been impressed and distressed at how the Net can spontaneously generates misinformation. Steve Jackson has spent untold hours correcting errors about him, his company, and the case on both the Net and more traditional news media.

The decision in the Steve Jackson Games case is clearly a significant victory for computer users, especially BBS operators and subscribers. I hope to give a simple and clear explanation for the intelligent non-lawyer of the legal issues raised by the case, and the significance and limitations of the court's decision.

The facts. By now, most people interested in the case are familiar with the basic facts: On March 1, 1990, the Secret Service, in an early-morning raid, searched the offices of Steve Jackson Games. The agents kept the employees out of the offices until the afternoon, and took the company's BBS -- called

"Illuminati" -- along with an employee's work computer, other computer equipment, and hundreds and hundreds of floppy disks. They took all the recent versions of a soon-to-be-published game book, "GURPS Cyberpunk," including big parts of the draft which were publicly available on Illuminati.

On March 2, Steve Jackson tried to get copies of the seized files back from the Secret Service. He was treated badly, and given only a handful of files from one office computer. He was not allowed to touch the Illuminati computer, or copy any of its files.

Steve Jackson Games took a nosedive, and barely avoided going out of business. According to Jackson, eight employees lost their jobs on account of the Secret Service raid, and the company lost many thousands of dollars in sales. It is again a busy enterprise, no thanks to the Secret Service (although they tried to take credit, pointing to the supposedly wonderful publicity their raid produced).

After months of pestering, including pressure by lawyers and Senator Lloyd Bentsen (now, as Treasury Secretary, the Secret Service's boss) the Secret Service returned most of the equipment taken, some of it much the worse for wear.

By then, Steve Jackson had restarted Illuminati on a different computer. When the old Illuminati computer was finally given back, Jackson turned it on -- and saw that all the electronic mail which had been on the board on March 1 was gone! Wayne Bell, WWIV developer and guru, was called in. He gave us invaluable (and free) help evaluating the condition of the files. He concluded, and testified firmly at trial, that during the week of March 20, 1990, when the Secret Service still had Illuminati, the BBS was run, and every piece of e-mail was individually accessed and deleted. The Illuminati files the Secret Service had returned to Steve Jackson left irrefutable electronic traces of what had been done -- even I could understand how the condition and dates of the e-mail files showed what had happened, and when.

The Lawsuit

Sueing the federal government and its agents is never a simple thing. The United States can only be sued when it consents. Lawsuits against individual agents face big legal hurdles erected to protect government officials from fear of a tidal wave of lawsuits.

Amazing as it may sound, you cannot sue the United States (or any federal agency) for money damages for violating your constitutional rights. You can sue individual federal agents, though. If you do, you have to get past a defense called "qualified immunity" which basically means you have to show that the officials violated "clearly established" constitutional law. For reasons I can't explain briefly, "qualified immunity" often creates a vicious circle in civil rights litigation, where the substance of constitutional law is never established because the court never has determine the Constitution's scope, only whether the law was "clearly established" at the time of the violation.

The strongest remedies for federal overstepping are often statutes which allow direct suit against the United States or federal agencies (although these are less dramatic than the Constitution). Fortunately, these statutes were available to Steve Jackson and the three Illuminati users who joined him in his suit against the Secret Service.

The Legal Claims

The Steve Jackson Games case was a lot of things to a lot of people. I saw the case as having two basic goals: (1) to redress the suppression of the public expression embodied in Steve Jackson's publications (including his publication via BBS) and thereby compensate the company for the damage unnecessarily done by the raid, and (2) to redress the violation of the privacy of the BBS users, and the less tangible harm they suffered.

The individual government agents involved in the raid were sued for constitutional violations -- the First and Fourth Amendments. The Secret Service was sued under two important laws which embody the same principles as the First and Fourth Amendments -- the Privacy Protection Act of 1980 and provisions of the Electronic Communications Privacy Act of 1986. There were other claims, but these were the core.

After the case was pending a year and a half and all discovery completed, the government moved to have the claims against the individual defendants dismissed, claiming qualified immunity. This motion (usually brought early in a case) guaranteed that the trial would be delayed by over a year, because even if the government lost its motion, the individuals could immediately appeal. In December, 1992, the tactical decision was made to drop those claims, rather than suffer the delay, and proceed promptly to trial

on the claims against the Secret Service itself.

The Privacy Protection Act of 1980

In the late 1970's the Stanford Daily was subjected to a fishing expedition conducted by police officers in the Stanford Daily's newsroom. The police were looking for notes and photos of a demonstration the newspaper had covered for a story, hoping the newspaper's files would identify suspects. The Supreme Court held in 1979 that the newspaper had no separate First Amendment right protecting it from searches and seizures of its reporters' notes and photographs if they were "evidence" of a crime the paper had covered -- even when the newspaper was not under any suspicion itself. Congress responded in 1980 with the Privacy Protection Act, which, until Steve Jackson came along, was distinguished mostly by its lack of interpretation by courts.

The Act's wording is rather obtuse, but basically it enacts a "subpoena only" rule for publishers -- law enforcement officials are not allowed to search for evidence of crimes in publishers' offices, or more accurately, they may not "search for or seize" publishers' "work product" or "documentary materials", essentially draft of publications, writers' notes, and such. To get such material, the police must subpoena them, not with the much more disruptive search warrant. Every BBS sysop should read this act, located at 42 U.S.C. 2000aa in the law books, because I can't fully explain it here.

The Act is quite broad, protecting from searches and seizures the work product and documentary materials of anyone who has "a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication ..." It also has a big exception -- if the publisher is the person suspected in the criminal investigation.

The Electronic Communications Privacy Act

Two provisions of the Electronic Communications Privacy Act (or ECPA) were paramount in the suit. The plaintiffs claimed the Secret Service violated two provisions -- one prohibiting unjustified "disclosure and use" of e-mail (18 U.S.C. Sec. 2703; the other prohibiting "interception" of e-mail (18 U.S.C. Sec. 2511(1)).

The parties' positions were fairly simple, and laid out well before trial. As for the Privacy Protection Act, Steve Jackson claimed that his company's publications, both in book form and on Illuminati, were obviously "work product" protected by the Act, and

the government had no right to seize them, and therefore owed him money for the damage the raid caused his business. The government replied claiming that (1) Steve Jackson Games' products are not the type of publications protected by the PPA; and anyway, (2) the Secret Service didn't know that Steve Jackson Games was a publisher when it raided its offices; and even then, (3) the Secret Service didn't mean to take the books, the books just came along when the computers and disks were taken.

As for the e-mail, Steve Jackson and the other BBS users claimed that the seizure, disclosure, and deletion of the e-mail was both an unlawful "disclosure and use," and an "interception" of electronic communications in violation of the ECPA. The Secret Service replied that (1) there was no "interception" because the e-mail was just sitting there on the hard drive, not moving; and (2) the Secret Service didn't read the mail, but if it did, it was acting in good faith, because it had a search warrant authorizing it so seize Steve Jackson Games' "computers" and to read their contents.

The Trial

When the individual defendants were dropped, the case quickly went to trial. The plaintiffs opened their case on January 29, 1993. The trial took the better part of four days; the witnesses included now-familiar names: Timothy Foley and Barbara Golden of the Secret Service, William Cook, formerly of the U.S. Attorney's office in Chicago, Henry Kluepfel of Bellcore, Steve Jackson and the BBS users Elizabeth McCoy, Walter Milliken and Steffan O'Sullivan, and WWIV master Wayne Bell.

At trial, Judge Sparks was introduced to the labyrinthine E911 investigation. We also set up and ran Illuminati as it looked on March 1, 1990, and Steve Jackson walked Judge Sparks through his BBS, lingering on discussion areas such as "GURPS Old West" to give the Judge a taste of the scope and breadth of BBS publication and communication which the Secret Service had shut down. The judge appeared upset by the callous and suspicious manner in which the Secret Service had treated Steve Jackson, and with the Service's apparent disregard for the effects the raid might have on the company.

The Decision

Judge Sparks decided the case in February, 1993, in a long written opinion. The full text of the opinion is available on the Internet at ftp.eff.org, and on Illuminati itself.

I recommend all sysops and BBS users to read it,
as it is one of the very few legal rulings specifically addressing
bulletin boards and electronic mail.

First, the bad news: Judge Sparks accepted the government's argument that the seizure of the BBS was not an "interception" of the e-mail, even mail that had not yet been read. Essentially, he decided that the definition of "interception" implicitly means "contemporaneous with the transmission"; that is, for there to be an interception, the government must position itself in the data stream, like a conventional wiretap. Since the e-mail was temporarily stored on the BBS hard drive, he held there was no contemporaneous interception.

Ruling that there was no interception means two things. First, the plaintiffs did not receive the $10,000 minimum damages a violation of the "interception" law provides, even though the judge found the Secret Service had not acted in good faith. More importantly, it lowers the standard for seizing BBS e-mail -- and threatens to lower the standard for the seizure of all electronic communications which reside long enough in computer memory to be seized (which is most all computer communications, as far as I understand it). To "intercept" wire communications you need a court order, not just a routine search warrant. This ruling (which technically only applies in the Western District of Texas) means law enforcement is not limited in its seizure of BBSs by the higher standards required of wiretapping.

Now, the good news: the plaintiffs won the "disclosure and use" argument under the ECPA, getting back most of what was lost in the "interception" decision. First, Judge Sparks found the obvious: that while the Secret Service had Illuminati they or their agents read and deleted all the e-mail on Illuminati, including the plaintiffs' mail -- persons the Secret Service admittedly having no reason at all to suspect of any illegal activity.

Next, he rejected the Secret Service's argument that its agents were acting in "good faith." While he didn't list all the reasons, quite a few are supported by the evidence: the Secret Service's investigation was "sloppy", he said, and there was no attempt to find out what Steve Jackson Games did as a business; the Secret Service was told the day of the raid that the company was a "publisher," and refused to make copies or return the files for months after they were done reviewing them; and the Secret Service

apparently allowed the private mail of dozens of entirely innocent and unsuspecting people to be read and trashed.

The judge ruled that Steve Jackson, his company, and the three Illuminati users who joined Jackson in the suit were each entitled to an $1,000 award from the government, as provided by the ECPA.

The Privacy Protection Act was pretty much a clean sweep. While the judge and Steve Jackson still differ over how much money the raid cost the company, the court's ruling was squarely in Jackson's favor on the law. Although unconventional, the court found that Steve Jackson Games' publications were clearly covered by the Act, should not have been seized, and should have been promptly returned.

At trial, the Secret Service agents had freely admitted they knew nothing about the Act. Former U.S. Attorney William Cook claimed he knew about it before the raid, but decided (without any investigation) that Steve Jackson Games wasn't covered. The Privacy Protection Act (unlike the ECPA) allows no "good faith" excuses, anyway, and since the Secret Service was repeatedly told on March 1 and afterwards that the company was a publishing business there was no defense for the seizure of "GURPS Cyberpunk" or the other book drafts. Most of the over $50,000 awarded in damages was due to the violation of the Privacy Protection Act.

Steve Jackson Games publishes traditional books and magazines, with printed paper pages. Is the BBS operator who publishes only on-line articles protected, too? It's a question Judge Sparks did not need to address directly, but his opinion can and should be read to include the on-line publisher. The court's opinion includes the BBS files as material improperly seized, and the Act specifically includes work product in electronic form. Publishing via BBSs has become just like publishing a "newspaper, book, or other form of publication..." -- the only source of news many people get.

If the Privacy Protection Act is broadly understood to encompass electronic publishing (as it should) it should provide meaningful protection to innocent sysops whose boards may be used by some for illegal purposes. It should prevent the "preventative detention" of BBSs -- where boards are seized in investigations and held indefinitely -- which seems to be one crude means used to attack suspected criminal activity without bothering to actually prosecute a case. It should also force law enforcement to consider

who the actual suspect is -- for instance, in the recent spate of seizures of BBSs for suspected copyright violations. The Privacy Protection Act should prevent law enforcement from seizing a sysop's board who is not suspected in engaging or condoning illegal activity.

Those of you who have followed this case will note how little significance I've given the "Phrack" investigation and the overvaluation of the E911 document. Of course the Secret Service misunderstood or exaggerated the importance of the purloined E911 document, and were chasing imaginary goblins.

The real significance of the Steve Jackson Games case, however, was not knocking holes in that one investigation (the Neidorf trial effectively did that), but taking a solid step to set firm, discernable limits for criminal investigations involving computer communication. To focus on the specific foibles of the E911 investigation is to miss the importance of what the Secret Service really did wrong. Out of ignorance or callousness, they ignored the legal rights of people not even suspected of crimes; people who simply shared common electronic space. There are and will continue to be legitimate computer-crime investigations. The closeness that people live in Cyberspace, though, means the government must learn ways to conduct investigations without violating the rights of all the innocent members of the on-line community. In March 1990, the Privacy Protection Act said that Steve Jackson could write and publish his books without having them seized; the Secret Service didn't know that. In 1990, the Illuminati users had the right not to have their e-mail seized and read without at least being suspected of a crime; the Secret Service apparently didn't know that, either. Now they do, and hopefully the word will spread to other government agencies, too.

(As of this writing, there is still no decision whether the Secret Service (or Steve Jackson, for that matter) will appeal Judge Spark's decision.)

The Constitution in Cyberspace

by Laurence H. Tribe

Tyler Professor of Constitutional Law, Harvard Law School

PREPARED REMARKS

KEYNOTE ADDRESS AT ThE
FIRST CONFERENCE ON COMPUTERS, FREEDOM & PRIVACY

  Arrangements to publish printed Proceedings of the First Conference on Computers, Freedom & Privacy are near completion. Audiotape and videotape versions are also being arranged.
  A later version of this file on the WELL (Sausalito, California) will include ordering details. Or, for details, or to propose other distribution alternatives, contact Jim Warren, CFP Chair,345 Swett Rd., Woodside CA 94062; voice:(415)851-7075; fax:(415)851-2814; e-mail:jwarren@well.sf.ca.us.[4/19/91]

[These were the author's *prepared* remarks.
  A transcript of Professor Tribe's March 26th comments at the Conference (which expanded slightly on several points herein) will be uploaded onto the WELL as soon as it is transcribed from the audio tapes and proofed against the audio and/or videotapes.]

"The Constitution in Cyberspace:

Law and Liberty Beyond the Electronic Frontier"

by Laurence H. Tribe

Tyler Professor of Constitutional Law, Harvard Law School.

Professor Tribe is the author, most recently, of
"On Reading the Constitution" (Harvard University Press,
Cambridge, MA, 1991).

Introduction

My topic is how to "map" the text and structure of our Constitution onto the texture and topology of "cyberspace". That's the term coined by cyberpunk novelist William Gibson, which many now use to describe the "place" -- a place without physical walls or even physical dimensions -- where ordinary telephone conversations "happen," where voice-mail and e-mail messages are stored and sent back and forth, and where computer-generated graphics are transmitted and transformed, all in the form of interactions, some real-time and some delayed, among countless users, and between users and the computer itself

Some use the "cyberspace" concept to designate fantasy worlds or "virtual realities" of the sort Gibson described in his novel *Neuromancer*, in which people can essentially turn their minds into computer peripherals capable of perceiving and exploring the data matrix. The whole idea of "virtual reality," of course, strikes a slightly odd note. As one of Lily Tomlin's most memorable characters once asked, "What's reality, anyway, but a collective hunch?" Work in this field tends to be done largely by people who share the famous observation that reality is overrated!

However that may be, "cyberspace" connotes to some users the sorts of technologies that people in Silicon Valley (like Jaron Lanier at VPL Research, for instance) work on when they try to develop "virtual racquetball" for the disabled, computer-aided design systems that allow architects to walk through "virtual buildings" and remodel them *before* they are built, "virtual conferencing" for business meetings, or maybe someday even "virtual day care centers" for latchkey children. The user snaps on a pair of goggles hooked up to a high-powered computer terminal, puts on a special set of gloves (and perhaps other gear) wired into the same computer system, and, looking a little bit like Darth Vader, pretty much steps into a computer-driven, drug-free, 3-dimensional, interactive, infinitely expandable hallucination complete with sight, sound and touch -- allowing the user literally to move

through, and experience, information.

I'm using the term "cyberspace" much more broadly, as many have lately. I'm using it to encompass the full array of computer-mediated audio and/or video interactions that are already widely dispersed in modern societies -- from things as ubiquitous as the ordinary telephone, to things that are still coming on-line like computer bulletin boards and networks like Prodigy, or like the WELL ("Whole Earth 'Lectronic Link"), based here in San Francisco. My topic, broadly put, is the implications of that rapidly expanding array for our constitutional order. It is a constitutional order that tends to carve up the social, legal, and political universe along lines of "physical place" or "temporal proximity." The critical thing to note is that these very lines, in cyberspace, either get bent out of shape or fade out altogether. The question, then, becomes: when the lines along which our Constitution is drawn warp or vanish, what happens to the Constitution itself?

Setting the Stage

To set the stage with a perhaps unfamiliar example, consider a decision handed down nine months ago, *Maryland v. Craig*, where the U.S. Supreme Court upheld the power of a state to put an alleged child abuser on trial with the defendant's accuser testifying not in the defendant's presence but by one-way, closed-circuit television. The Sixth Amendment, which of course antedated television by a century and a half, says: "In all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the witnesses against him." Justice O'Connor wrote for a bare majority of five Justices that the state's procedures nonetheless struck a fair balance between costs to the accused and benefits to the victim and to society as a whole. Justice Scalia, joined by the three "liberals" then on the Court (Justices Brennan, Marshall and Stevens), dissented from that cost-benefit approach to interpreting the Sixth Amendment. He wrote:

> The Court has convincingly proved that the Maryland procedure serves a valid interest, and gives the defendant virtually everything the Confrontation Clause guarantees (everything, that is, except confrontation). I am persuaded, therefore, that the Maryland procedure is virtually constitutional. Since it is not, however, actually constitutional I [dissent].
>
> Could it be that the high-tech, closed-circuit TV context,

almost as familiar to the Court's youngest Justice as to his even younger law clerks, might've had some bearing on Justice Scalia's sly invocation of "virtual" constitutional reality? Even if Justice Scalia wasn't making a pun on "virtual reality," and I suspect he wasn't, his dissenting opinion about the Confrontation Clause requires *us* to "confront" the recurring puzzle of how constitutional provisions written two centuries ago should be construed and applied in ever-changing circumstances.

Should contemporary society's technology-driven cost-benefit fixation be allowed to water down the old-fashioned value of direct confrontation that the Constitution seemingly enshrined as basic? I would hope not. In that respect, I find myself in complete agreement with Justice Scalia.

But new technological possibilities for seeing your accuser clearly without having your accuser see you at all -- possibilities for sparing the accuser any discomfort in ways that the accuser couldn't be spared before one-way mirrors or closed-circuit TVs were developed -- *should* lead us at least to ask ourselves whether *two*-way confrontation, in which your accuser is supposed to be made uncomfortable, and thus less likely to lie, really *is* the core value of the Confrontation Clause. If so, "virtual" confrontation should be held constitutionally insufficient. If not -- if the core value served by the Confrontation Clause is just the ability to *watch* your accuser say that you did it -- then "virtual" confrontation should suffice. New technologies should lead us to look more closely at just *what values* the Constitution seeks to preserve. New technologies should *not* lead us to react reflexively *either way* -- either by assuming that technologies the Framers didn't know about make their concerns and values obsolete, or by assuming that those new technologies couldn't possibly provide new ways out of old dilemmas and therefore should be ignored altogether.

The one-way mirror yields a fitting metaphor for the task we confront. As the Supreme Court said in a different context several years ago, "The mirror image presented [here] requires us to step through an analytical looking glass to resolve it." (*NCAA v. Tarkanian*, 109 S. Ct. at 462.) The world in which the Sixth Amendment's Confrontation Clause was written and ratified was a world in which "being confronted with" your accuser *necessarily* meant a simultaneous physical confrontation so that your accuser had to *perceive* you being accused by him. Closed-circuit television and one-way mirrors changed all that by *decoupling* those two dimensions of confrontation, marking a shift in the conditions of information-transfer that is in many ways typical of cyberspace.

What does that sort of shift mean for constitutional analysis? A common way to react is to treat the pattern as it existed *prior* to the new technology (the pattern in which doing "A" necessarily

included doing "B") as essentially arbitrary or accidental. Taking this approach, once the technological change makes it possible to do "A" *without* "B" -- to see your accuser without having him or her see you, or to read someone's mail without her knowing it, to switch examples -- one concludes that the "old" Constitution's inclusion of "B" is irrelevant; one concludes that it is enough for the government to guarantee "A" alone. Sometimes that will be the case; but it's vital to understand that, sometimes, it won't be.

A characteristic feature of modernity is the subordination of purpose to accident -- an acute appreciation of just how contingent and coincidental the connections we are taught to make often are. We understand, as moderns, that many of the ways we carve up and organize the world reflect what our social history and cultural heritage, and perhaps our neurological wiring, bring to the world, and not some irreducible "way things are." A wonderful example comes from a 1966 essay by Jorge Louis Borges, "Other Inquisitions." There, the essayist describes the following taxonomy of the animal kingdom, which he purports to trace to an ancient Chinese encyclopedia entitled *The Celestial Emporium of Benevolent Knowledge*:

> On those remote pages it is written that animals are divided into:
>
> (a) those belonging to the Emperor
> (b) those that are embalmed
> (c) those that are trained
> (d) suckling pigs
> (e) mermaids
> (f) fabulous ones
> (g) stray dogs
> (h) those that are included in this classification
> (i) those that tremble as if they were mad
> (j) innumerable ones
> (k) those drawn with a very fine camel's hair brush
> (l) others
> (m) those that have just broken a water pitcher
> (n) those that, from a great distance, resemble flies

Contemporary writers from Michel Foucault, in *The Archaeology of Knowledge*, through George Lakoff, in *Women, Fire, and Dangerous Things*, use Borges' Chinese encyclopedia to illustrate a range of different propositions, but the *core* proposition is the supposed arbitrariness -- the political character, in a sense -- of all culturally imposed categories.

At one level, that proposition expresses a profound truth and may encourage humility by combating cultural imperialism. At another level, though, the proposition tells a dangerous lie: it suggests that we have descended into the nihilism that so obsessed Nietzsche and other thinkers -- a world where *everything* is relative, all lines are up for grabs, all principles and

connections are just matters of purely subjective preference or, worse still, arbitrary convention. Whether we believe that killing animals for food is wrong, for example, becomes a question indistinguishable from whether we happen to enjoy eating beans, rice and tofu.

This is a particularly pernicious notion in a era when we pass more and more of our lives in cyberspace, a place where, almost by definition, our most familiar landmarks are rearranged or disappear altogether -- because there is a pervasive tendency, even (and perhaps especially) among the most enlightened, to forget that the human values and ideals to which we commit ourselves may indeed be universal and need not depend on how our particular cultures, or our latest technologies, carve up the universe we inhabit. It was my very wise colleague from Yale, the late Art Leff, who once observed that, even in a world without an agreed-upon God, we can still agree -- even if we can't "prove" mathematically -- that "napalming babies is wrong."

The Constitution's core values, I'm convinced, need not be transmogrified, or metamorphosed into oblivion, in the dim recesses of cyberspace. But to say that they *need* not be lost there is hardly to predict that they *will* not be. On the contrary, without further thought and awareness of the kind this conference might provide, the danger is clear and present that they *will* be.

The "event horizon" against which this transformation might occur is already plainly visible:

Electronic trespassers like Kevin Mitnik don't stop with cracking pay phones, but break into NORAD -- the North American Defense Command computer in Colorado Springs -- not in a *WarGames* movie, but in real life.

Less challenging to national security but more ubiquitously threatening, computer crackers download everyman's credit history from institutions like TRW; start charging phone calls (and more) to everyman's number; set loose "worm" programs that shut down thousands of linked computers; and spread "computer viruses" through everyman's work or home PC.

It is not only the government that feels threatened by "computer crime"; both the owners and the users of private information services, computer bulletin boards, gateways, and networks feel equally vulnerable to this new breed of invisible trespasser. The response from the many who sense danger has been swift, and often brutal, as a few examples illustrate.

Last March, U.S. Secret Service agents staged a surprise raid on Steve Jackson Games, a small games manufacturer in Austin, Texas, and seized all paper and electronic drafts of its newest fantasy role-playing game, *GURPS[reg.t.m.] Cyberpunk*, calling the game a "handbook for computer crime."

By last Spring, up to one quarter of the U.S. Treasury

Department's investigators had become involved in a project of eavesdropping on computer bulletin boards, apparently tracking notorious hackers like "Acid Phreak" and "Phiber Optik" through what one journalist dubbed "the dark canyons of cyberspace."

Last May, in the now famous (or infamous) "Operation Sun Devil," more than 150 secret service agents teamed up with state and local law enforcement agencies, and with security personnel from AT&T, American Express, U.S. Sprint, and a number of the regional Bell telephone companies, armed themselves with over two dozen search warrants and more than a few guns, and seized 42 computers and 23,000 floppy discs in 14 cities from New York to Texas. Their target: a loose-knit group of people in their teens and twenties, dubbed the "Legion of Doom."

I am not describing an Indiana Jones movie. I'm talking about America in the 1990s.

The Problem

The Constitution's architecture can too easily come to seem quaintly irrelevant, or at least impossible to take very seriously, in the world as reconstituted by the microchip. I propose today to canvass five axioms of our constitutional law -- five basic assumptions that I believe shape the way American constitutional scholars and judges view legal issues -- and to examine how they can adapt to the cyberspace age. My conclusion (and I will try not to give away too much of the punch line here) is that the Framers of our Constitution were very wise indeed. They bequeathed us a framework for all seasons, a truly astonishing document whose principles are suitable for all times and all technological landscapes.

Axiom 1:
There is a Vital Difference
Between Government and Private Action

The first axiom I will discuss is the proposition that the Constitution, with the sole exception of the Thirteenth Amendment prohibiting slavery, regulates action by the *government* rather than the conduct of *private* individuals and groups. In an article I wrote in the Harvard Law Review in November 1989 on "The Curvature of Constitutional Space," I discussed the Constitution's metaphor-morphosis from a Newtonian to an Einsteinian and Heisenbergian paradigm. It was common, early in our history, to see the Constitution as "Newtonian in design with its carefully counterpoised forces and counterforces, its [geographical and institutional] checks and balances." (103 *Harv. L. Rev.* at 3.)

Indeed, in many ways contemporary constitutional law is still trapped within and stunted by that paradigm. But today at least some post-modern constitutionalists tend to think and talk in the language of relativity, quantum mechanics, and chaos theory. This may quite naturally suggest to some observers that the Constitution's basic strategy of decentralizing and diffusing power by constraining and fragmenting governmental authority in particular has been rendered obsolete.

The institutional separation of powers among the three federal branches of government, the geographical division of authority between the federal government and the fifty state governments, the recognition of national boundaries, and, above all, the sharp distinction between the public and private spheres, become easy to deride as relics of a simpler, pre-computer age. Thus Eli Noam, in the First Ithiel de Sola Pool Memorial Lecture, delivered last October at MIT, notes that computer networks and network associations acquire quasi-governmental powers as they necessarily take on such tasks as mediating their members' conflicting interests, establishing cost shares, creating their own rules of admission and access and expulsion, even establishing their own *de facto* taxing mechanisms. In Professor Noam's words, "networks become political entities," global nets that respect no state or local boundaries. Restrictions on the use of information in one country (to protect privacy, for example) tend to lead to export of that information to other countries, where it can be analyzed and then used on a selective basis in the country attempting to restrict it. "Data havens" reminiscent of the role played by the Swiss in banking may emerge, with few restrictions on the storage and manipulation of information.

A tempting conclusion is that, to protect the free speech and other rights of *users* in such private networks, judges must treat these networks not as associations that have rights of their own *against* the government but as virtual "governments" in themselves -- as entities against which individual rights must be defended in the Constitution's name. Such a conclusion would be misleadingly simplistic. There are circumstances, of course, when non-governmental bodies like privately owned "company towns" or even huge shopping malls should be subjected to legislative and administrative controls by democratically accountable entities, or even to judicial controls as though they were arms of the state -- but that may be as true (or as false) of multinational corporations or foundations, or transnational religious organizations, or even small-town communities, as it is of computer-mediated networks. It's a fallacy to suppose that, just because a computer bulletin board or network or gateway is *something like* a shopping mall, government has as much constitutional duty -- or even authority -- to guarantee open public access to such a network as it has to

guarantee open public access to a privately owned shopping center like the one involved in the U.S. Supreme Court's famous *PruneYard Shopping Center* decision of 1980, arising from nearby San Jose.

The rules of law, both statutory and judge-made, through which each state *allocates* private powers and responsibilities themselves represent characteristic forms of government action. That's why a state's rules for imposing liability on private publishers, or for deciding which private contracts to enforce and which ones to invalidate, are all subject to scrutiny for their consistency with the federal Constitution. But as a general proposition it is only what *governments* do, either through such rules or through the actions of public officials, that the United States Constitution constrains. And nothing about any new technology suddenly erases the Constitution's enduring value of restraining *government* above all else, and of protecting all private groups, large and small, from government.

It's true that certain technologies may become socially indispensable -- so that equal or at least minimal access to basic computer power, for example, might be as significant a constitutional goal as equal or at least minimal access to the franchise, or to dispute resolution through the judicial system, or to elementary and secondary education. But all this means (or should mean) is that the Constitution's constraints on government must at times take the form of imposing *affirmative duties* to assure access rather than merely enforcing *negative prohibitions* against designated sorts of invasion or intrusion.

Today, for example, the government is under an affirmative obligation to open up criminal trials to the press and the public, at least where there has not been a particularized finding that such openness would disrupt the proceedings. The government is also under an affirmative obligation to provide free legal assistance for indigent criminal defendants, to assure speedy trials, to underwrite the cost of counting ballots at election time, and to desegregate previously segregated school systems. But these occasional affirmative obligations don't, or shouldn't, mean that the Constitution's axiomatic division between the realm of public power and the realm of private life should be jettisoned.

Nor would the "indispensability" of information technologies provide a license for government to impose strict content, access, pricing, and other types of regulation. *Books* are indispensable to most of us, for example -- but it doesn't follow that government should therefore be able to regulate the content of what goes onto the shelves of *bookstores*. The right of a private bookstore owner to decide which books to stock and which to discard, which books to display openly and which to store in limited access areas, should remain inviolate. And note, incidentally, that this needn't make the bookstore owner a "publisher" who is liable for the words

printed in the books on her shelves. It's a common fallacy to imagine that the moment a computer gateway or bulletin board begins to exercise powers of selection to control who may be on line, it must automatically assume the responsibilities of a newscaster, a broadcaster, or an author. For computer gateways and bulletin boards are really the "bookstores" of cyberspace; most of them organize and present information in a computer format, rather than generating more information content of their own.

Axiom 2:
The Constitutional Boundaries of Private Property and Personality Depend on Variables Deeper Than *Social Utility and Technological Feasibility*

The second constitutional axiom, one closely related to the private-public distinction of the first axiom, is that a person's mind, body, and property belong *to that person* and not to the public as a whole. Some believe that cyberspace challenges that axiom because its entire premise lies in the existence of computers tied to electronic transmission networks that process digital information. Because such information can be easily replicated in series of "1"s and "0"s, anything that anyone has come up with in virtual reality can be infinitely reproduced. I can log on to a computer library, copy a "virtual book" to my computer disk, and send a copy to your computer without creating a gap on anyone's bookshelf. The same is true of valuable computer programs, costing hundreds of dollars, creating serious piracy problems. This feature leads some, like Richard Stallman of the Free Software Foundation, to argue that in cyberspace everything should be free -- that information can't be owned. Others, of course, argue that copyright and patent protections of various kinds are needed in order for there to be incentives to create "cyberspace property" in the first place.

Needless to say, there are lively debates about what the optimal incentive package should be as a matter of legislative and social policy. But the only *constitutional* issue, at bottom, isn't the utilitarian or instrumental selection of an optimal policy. Social judgments about what ought to be subject to individual appropriation, in the sense used by John Locke and Robert Nozick, and what ought to remain in the open public domain, are first and foremost *political* decisions.

To be sure, there are some constitutional constraints on these political decisions. The Constitution does not permit anything and everything to be made into a *private commodity*. Votes, for example, theoretically cannot be bought and sold. Whether the Constitution itself should be read (or amended) so as to permit all

basic medical care, shelter, nutrition, legal assistance and, indeed, computerized information services, to be treated as mere commodities, available only to the highest bidder, are all terribly hard questions -- as the Eastern Europeans are now discovering as they attempt to draft their own constitutions. But these are not questions that should ever be confused with issues of what is technologically possible, about what is realistically enforceable, or about what is socially desirable.

Similarly, the Constitution does not permit anything and everything to be *socialized* and made into a public good available to whoever needs or "deserves" it most. I would hope, for example, that the government could not use its powers of eminent domain to "take" live body parts like eyes or kidneys or brain tissue for those who need transplants and would be expected to lead particularly productive lives. In any event, I feel certain that whatever constitutional right each of us has to inhabit his or her own body and to hold onto his or her own thoughts and creations should not depend solely on cost-benefit calculations, or on the availability of technological methods for painlessly effecting transfers or for creating good artificial substitutes.

Axiom 3:
Government May Not Control Information Content

A third constitutional axiom, like the first two, reflects a deep respect for the integrity of each individual and a healthy skepticism toward government. The axiom is that, although information and ideas have real effects in the social world, it's not up to government to pick and choose for us in terms of the *content* of that information or the *value* of those ideas.

This notion is sometimes mistakenly reduced to the naive child's ditty that "sticks and stones may break my bones, but words can never hurt me." Anybody who's ever been called something awful by children in a schoolyard knows better than to believe any such thing. The real basis for First Amendment values isn't the false premise that information and ideas have no real impact, but the belief that information and ideas are *too important* to entrust to any government censor or overseer.

If we keep that in mind, and *only* if we keep that in mind, will we be able to see through the tempting argument that, in the Information Age, free speech is a luxury we can no longer afford. That argument becomes especially tempting in the context of cyberspace, where sequences of "0"s and "1"s may become virtual life forms. Computer "viruses" roam the information nets, attaching themselves to various programs and screwing up computer facilities. Creation of a computer virus involves writing a

program; the program then replicates itself and mutates. The electronic code involved is very much like DNA. If information content is "speech," and if the First Amendment is to apply in cyberspace, then mustn't these viruses be "speech" -- and mustn't their writing and dissemination be constitutionally protected? To avoid that nightmarish outcome, mustn't we say that the First Amendment is *inapplicable* to cyberspace?

The answer is no. Speech is protected, but deliberately yelling "Boo!" at a cardiac patient may still be prosecuted as murder. Free speech is a constitutional right, but handing a bank teller a hold-up note that says, "Your money or your life," may still be punished as robbery. Stealing someone's diary may be punished as theft -- even if you intend to publish it in book form. And the Supreme Court, over the past fifteen years, has gradually brought advertising within the ambit of protected expression without preventing the government from protecting consumers from deceptive advertising. The lesson, in short, is that constitutional principles are subtle enough to bend to such concerns. They needn't be broken or tossed out.

Axiom 4:
The Constitution is Founded on Normative Conceptions of Humanity That Advances *in Science and Technology Cannot "Disprove"*

A fourth constitutional axiom is that the human spirit is something beyond a physical information processor. That axiom, which regards human thought processes as not fully reducible to the operations of a computer program, however complex, must not be confused with the silly view that, because computer operations involve nothing more than the manipulation of "on" and "off" states of myriad microchips, it somehow follows that government control or outright seizure of computers and computer programs threatens no First Amendment rights because human thought processes are not directly involved. To say that would be like saying that government confiscation of a newspaper's printing press and tomorrow morning's copy has nothing to do with speech but involves only a taking of metal, paper, and ink. Particularly if the seizure or the regulation is triggered by the content of the information being processed or transmitted, the First Amendment is of course fully involved. Yet this recognition that information processing by computer entails something far beyond the mebe sequencing of mechanical or chemical steps still leaves a potential gap between what computers can do internally and in communication with one another -- and what goes on within and between human minds. It is that gap to which this fourth axiom is addressed; the very

existence of any such gap is, as I'm sure you know, a matter of considerable controversy.

What if people like the mathematician and physicist Roger Penrose, author of *The Emperor's New Mind*, are wrong about human minds? In that provocative recent book, Penrose disagrees with those Artificial Intelligence, or AI, gurus who insist that it's only a matter of time until human thought and feeling can be perfectly simulated or even replicated by a series of purely physical operations -- that it's all just neurons firing and neurotransmitters flowing, all subject to perfect modeling in suitable computer systems. Would an adherent of that AI orthodoxy, someone whom Penrose fails to persuade, have to reject as irrelevant for cyberspace those constitutional protections that rest on the anti-AI premise that minds are *not* reducible to really fancy computers?

Consider, for example, the Fifth Amendment, which provides that "no person shall be . . . compelled in any criminal case to be a witness against himself." The Supreme Court has long held that suspects may be required, despite this protection, to provide evidence that is not "testimonial" in nature -- blood samples, for instance, or even exemplars of one's handwriting or voice. Last year, in a case called *Pennsylvania v. Muniz*, the Supreme Court held that answers to even simple questions like "When was your sixth birthday?" are testimonial because such a question, however straightforward, nevertheless calls for the product of mental activity and therefore uses the suspect's mind against him. But what if science could eventually describe thinking as a process no more complex than, say, riding a bike or digesting a meal? Might the progress of neurobiology and computer science eventually overthrow the premises of the *Muniz* decision?

I would hope not. For the Constitution's premises, properly understood, are *normative* rather than *descriptive*. The philosopher David Hume was right in teaching that no "ought" can ever be logically derived from an "is." If we should ever abandon the Constitution's protection for the distinctively and universally human, it won't be because robotics or genetic engineering or computer science have led us to deeper truths, but rather because they have seduced us into more profound confusions. Science and technology open options, create possibilities, suggest incompatibilities, generate threats. They do not alter what is "right" or what is "wrong." The fact that those notions are elusive and subject to endless debate need not make them totally contingent on contemporary technology.

Axiom 5:
Constitutional Principles Should Not

Vary With Accidents of Technology

In a sense, that's the fifth and final constitutional axiom I would urge upon this gathering: that the Constitution's norms, at their deepest level, must be invariant under merely *technological* transformations. Our constitutional law evolves through judicial interpretation, case by case, in a process of reasoning by analogy from precedent. At its best, that process is ideally suited to seeing beneath the surface and extracting deeper principles from prior decisions. At its worst, though, the same process can get bogged down in superficial aspects of preexisting examples, fixating upon unessential features while overlooking underlying principles and values.

When the Supreme Court in 1928 first confronted wiretapping and held in *Olmstead v. United States* that such wiretapping involved no "search" or "seizure" within the meaning of the Fourth Amendment's prohibition of "unreasonable searches and seizures," the majority of the Court reasoned that the Fourth Amendment "itself shows that the search is to be of material things -- the person, the house, his papers or his effects," and said that "there was no searching" when a suspect's phone was tapped because the Constitution's language "cannot be extended and expanded to include telephone wires reaching to the whole world from the defendant's house or office." After all, said the Court, the intervening wires "are not part of his house or office any more than are the highways along which they are stretched." Even to a law student in the 1960s, as you might imagine, that "reasoning" seemed amazingly artificial. Yet the *Olmstead* doctrine still survived.

It would be illuminating at this point to compare the Supreme Court's initial reaction to new technology in *Olmstead* with its initial reaction to new technology in *Maryland v. Craig*, the 1990 closed-circuit television case with which we began this discussion. In *Craig*, a majority of the Justices assumed that, when the 18th-century Framers of the Confrontation Clause included a guarantee of two-way *physical* confrontation, they did so solely because it had not yet become technologically feasible for the accused to look his accuser in the eye without having the accuser simultaneously watch the accused. Given that this technological obstacle has been removed, the majority assumed, one-way confrontation is now sufficient. It is enough that the accused not be subject to criminal conviction on the basis of statements made outside his presence.

In *Olmstead*, a majority of the Justices assumed that, when the 18th-century authors of the Fourth Amendment used language that sounded "physical" in guaranteeing against invasions of a person's dwelling or possessions, they did so not solely because *physical* invasions were at that time the only serious threats to personal

privacy, but for the separate and distinct reason that *intangible* invasions simply would not threaten any relevant dimension of Fourth Amendment privacy.

In a sense, *Olmstead* mindlessly read a new technology *out* of the Constitution, while *Craig* absent-mindedly read a new technology *into* the Constitution. But both decisions -- *Olmstead* and *Craig* -- had the structural effect of withholding the protections of the Bill of Rights from threats made possible by new information technologies. *Olmstead* did so by implausibly reading the Constitution's text as though it represented a deliberate decision not to extend protection to threats that 18th-century thinkers simply had not foreseen. *Craig* did so by somewhat more plausibly -- but still unthinkingly -- treating the Constitution's seemingly explicit coupling of two analytically distinct protections as reflecting a failure of technological foresight and imagination, rather than a deliberate value choice.

The *Craig* majority's approach appears to have been driven in part by an understandable sense of how a new information technology could directly protect a particularly sympathetic group, abused children, from a traumatic trial experience. The *Olmstead* majority's approach probably reflected both an exaggerated estimate of how difficult it would be to obtain wiretapping warrants even where fully justified, and an insufficient sense of how a new information technology could directly threaten all of us. Although both *Craig* and *Olmstead* reveal an inadequate consciousness about how new technologies interact with old values, *Craig* at least seems defensible even if misguided, while *Olmstead* seems just plain wrong.

Around 23 years ago, as a then-recent law school graduate serving as law clerk to Supreme Court Justice Potter Stewart, I found myself working on a case involving the government's electronic surveillance of a suspected criminal -- in the form of a tiny device attached to the outside of a public telephone booth. Because the invasion of the suspect's privacy was accomplished without physical trespass into a "constitutionally protected area," the Federal Government argued, relying on *Olmstead*, that there had been no "search" or "seizure," and therefore that the Fourth Amendment "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," simply did not apply.

At first, there were only four votes to overrule *Olmstead* and to hold the Fourth Amendment applicable to wiretapping and electronic eavesdropping. I'm proud to say that, as a 26-year-old kid, I had at least a little bit to do with changing that number from four to seven -- and with the argument, formally adopted by a seven-Justice majority in December 1967, that the Fourth Amendment "protects people, not places." (389 U.S. at 351.) In that

decision, *Katz v. United States*, the Supreme Court finally repudiated *Olmstead* and the many decisions that had relied upon it and reasoned that, given the role of electronic telecommunications in modern life, the First Amendment purposes of protecting *free speech* as well as the Fourth Amendment purposes of protecting *privacy* require treating as a "search" any invasion of a person's confidential telephone communications, with or without physical trespass.

Sadly, nine years later, in *Smith v. Maryland*, the Supreme Court retreated from the *Katz* principle by holding that no search occurs and therefore no warrant is needed when police, with the assistance of the telephone company, make use of a "pen register", a mechanical device placed on someone's phone line that records all numbers dialed from the phone and the times of dialing. The Supreme Court, over the dissents of Justices Stewart, Brennan, and Marshall, found no legitimate expectation of privacy in the numbers dialed, reasoning that the digits one dials are routinely recorded by the phone company for billing purposes. As Justice Stewart, the author of *Katz*, aptly pointed out, "that observation no more than describes the basic nature of telephone calls . . . . It is simply not enough to say, after *Katz*, that there is no legitimate expectation of privacy in the numbers dialed because the caller assumes the risk that the telephone company will expose them to the police." (442 U.S. at 746-747.) Today, the logic of *Smith* is being used to say that people have no expectation of privacy when they use their cordless telephones since they know or should knowgmn?^? that radio waves can be easily monitored!

It is easy to be pessimistic about the way in which the Supreme Court has reacted to technological change. In many respects, *Smith* is unfortunately more typical than *Katz* of the way the Court has behaved. For example, when movies were invented, and for several decades thereafter, the Court held that movie exhibitions were not entitled to First Amendment protection. When community access cable TV was born, the Court hindered municipal attempts to provide it at low cost by holding that rules requiring landlords to install small cable boxes on their apartment buildings amounted to a compensable taking of property. And in *Red Lion v. FCC*, decided twenty-two years ago but still not repudiated today, the Court ratified government control of TV and radio broadcast content with the dubious logic that the scarcity of the electromagnetic spectrum justified not merely government policies to auction off, randomly allocate, or otherwise ration the spectrum according to neutral rules, but also much more intrusive and content-based government regulation in the form of the so-called "fairness doctrine."

Although the Supreme Court and the lower federal courts have taken a somewhat more enlightened approach in dealing with cable

television, these decisions for the most part reveal a curious judicial blindness, as if the Constitution had to be reinvented with the birth of each new technology. Judges interpreting a late 18th century Bill of Rights tend to forget that, unless its *terms* are read in an evolving and dynamic way, its *values* will lose even the *static* protection they once enjoyed. Ironically, *fidelity* to original values requires *flexibility* of textual interpretation. It was Judge Robert Bork, not famous for his flexibility, who once urged this enlightened view upon then Judge (now Justice) Scalia, when the two of them sat as colleagues on the U.S. Court of Appeals for the D.C. Circuit.

Judicial error in this field tends to take the form of saying that, by using modern technology ranging from the telephone to the television to computers, we "assume the risk." But that typically begs the question. Justice Harlan, in a dissent penned two decades ago, wrote: "Since it is the task of the law to form and project, as well as mirror and reflect, we should not . . . merely recite . . . risks without examining the *desirability* of saddling them upon society." (*United States v. White*, 401 U.S. at 786). And, I would add, we should not merely recite risks without examining how imposing those risks comports with the Constitution's fundamental values of *freedom*, *privacy*, and *equality*.

Failing to examine just that issue is the basic error I believe federal courts and Congress have made:

* in regulating radio and TV broadcasting without adequate sensitivity to First Amendment values;

* in supposing that the selection and editing of video programs by cable operators might be less than a form of expression;

* in excluding telephone companies from cable and other information markets;

* in assuming that the processing of "O"s and "1"s by computers as they exchange data with one another is something less than "speech"; and

* in generally treating information processed electronically as though it were somehow less entitled to protection for that reason.

The lesson to be learned is that these choices and these mistakes are not dictated by the Constitution. They are decisions for us to make in interpreting that majestic charter, and in implementing the principles that the Constitution establishes.

Conclusion

If my own life as a lawyer and legal scholar could leave just one legacy, I'd like it to be the recognition that the Constitution *as a whole* "protects people, not places." If that is to come about, the Constitution as a whole must be read through a technologically transparent lens. That is, we must embrace, as a rule of construction or interpretation, a principle one might call the "cyberspace corollary." It would make a suitable Twenty-seventh Amendment to the Constitution, one befitting the 200th anniversary of the Bill of Rights. Whether adopted all at once as a constitutional amendment, or accepted gradually as a principle of interpretation that I believe should obtain even without any formal change in the Constitution's language, the corollary I would propose would do for *technology* in 1991 what I believe the Constitution's Ninth Amendment, adopted in 1791, was meant to do for *text*.

The Ninth Amendment says: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people." That amendment provides added support for the long-debated, but now largely accepted, "right of privacy" that the Supreme Court recognized in such decisions as the famous birth control case of 1965, *Griswold v. Connecticut*. The Ninth Amendment's simple message is: The *text* used by the Constitution's authors and ratifiers does not exhaust the values our Constitution recognizes. Perhaps a Twenty-seventh Amendment could convey a parallel and equally simple message: The *technologies* familiar to the Constitution's authors and ratifiers similarly do not exhaust the *threats* against which the Constitution's core values must be protected.

The most recent amendment, the twenty-sixth, adopted in 1971, extended the vote to 18-year-olds. It would be fitting, in a world where youth has been enfranchised, for a twenty-seventh amendment to spell a kind of "childhood's end" for constitutional law. The Twenty-seventh Amendment, to be proposed for at least serious debate in 1991, would read simply:

"This Constitution's protections for the freedoms of speech, press, petition, and assembly, and its protections against unreasonable searches and seizures and the deprivation of life, liberty, or property without due process of law, shall be construed as fully applicable without regard to the technological method or medium through which information content is generated, stored, altered, transmitted, or controlled."

[Note: The machine-readable original of this was provided by the author on a PC diskette in WordPerfect. It was reformatted to ASCII, appropriate for general network and computer access, by Jim Warren. Text that was underlined or boldface in the original copy was delimited by asterisks, and a registered trademark symbol was replaced by "reg.t.m.". Other than that, the text was as provided by the author.]

THE TOP TEN MEDIA ERRORS ABOUT THE SJ GAMES RAID

updated 10-12-94

As this story has developed, occasional errors crept into news stories - and many of them have taken on a life of their own. Some reporters, working from their clipping files, have turned out stories that are almost 100% free of facts. There are a lot of those floating around . . . but here are our Top Ten.

10. Steve Jackson Games is a computer game company.
No we're not. None of our games are computer games. We use computers to WRITE the games, like every other publisher in the '90s. The game that was seized, GURPS CYBERPUNK, was about computers. And we ran a computer BBS where people DISCUSSED games. But we're not a computer game company any more than George Bush is a gardener.

9. GURPS Cyberpunk is a computer game.
No it's not. Aieeeeee! It's a roleplaying game. It is not played on a computer. It's played on a table, with dice.

8. We're out of business.
No we're not. It's been reported that we are bankrupt, or filing for bankruptcy. It was very close - we DID have to lay off half our staff, and it was a while before we were out of the woods . . . but we're not dead.

7. We were raided by the FBI.
No we weren't. We were raided by the US Secret Service. The FBI had nothing to do with it. (In fact, when Bill Cook, the assistant US attorney named in our suit, was doing his "research," he talked to the FBI. They told him he didn't have a case. We have this from FBI sources!)

6. Some of our staff members were arrested by the Secret Service and charged with hacking.
No they weren't. No member of our staff was arrested, indicted, or charged. Nobody was even QUESTIONED after the day of the raid.

5. This was part of Operation Sun Devil.
No it wasn't. Sun Devil was a totally separate project, aimed at credit card fraud. Because it had a neat name, it got a lot of headlines. Since computers were involved, some reporters got the two confused. The Secret Service helped the confusion along by refusing to comment on what was, or wasn't part of Sun Devil. Sun Devil was not a "hacker"

investigation. So says Gail Thackeray, who was its spearhead.

4. The raid was after GURPS Cyberpunk.
No it wasn't. The Secret Service suspected one of our staffers of wrongdoing, using his computer at home. They had nothing connecting his alleged misdeeds with our office, but they raided us anyway, and took a lot of things. One of the things they took was the GURPS Cyberpunk manuscript. Their agents were very critical of it, and on March 2 in their office, one of them called it a "handbook for computer crime." Since their warrant was sealed, and they wouldn't comment, our best guess was that they were trying to suppress the book. They did suppress it, but apparently it was through bureaucratic inertia and stonewalling rather than because it was a target of the raid.

3. There was a hacker threat to sabotage the 911 system.
No there wasn't. This story has been cynically spread by phone company employees (who know better) and by Secret Service spokesmen (who probably believe it, because they still don't understand any of this). They're using this story to panic the media, to try to justify the illegal things they've done and the huge amount of money they've spent.
What happened was this: A student got access to a phone company computer and copied a text file - not a program. This file was nothing but administrative information, and was publicly available elsewhere. Bell South tried to value it at $79,000, but in court they admitted that they sold copies for under $20. There was no way this file could be used to hurt the 911 system, even if anybody had wanted to. To say otherwise shows an incredible ignorance of the facts. It's as though a banker claimed "This criminal made an illegal copy of the list of our Board of Directors. He can use that to break into our vault."

2. We have an employee named Lloyd Blankenship.
Loyd spells his name with one L.

And the Number One "false fact" ever reported about this story . . .

1. Steve Jackson Games is the second largest game company in the USA.
Don't we wish!

Texas Computer Crime Law

as passed by the Texas Legislature in 1994 . . .

TEXAS PENAL CODE
TITLE 7. OFFENSES AGAINST PROPERTY
CHAPTER 33. COMPUTER CRIMES

33.01. Definitions

In this chapter:

(1) "Access" means to approach, instruct, communicate with, store data in, retrieve or intercept data from, alter data or computer software in, or otherwise make use of any resource of a computer, computer system, or computer network.

(2) "Communications common carrier" means a person who owns or operates a telephone system in this state that includes equipment or facilities for the conveyance, transmission, or reception of communications and who receives compensation from persons who use that system.

(3) "Computer" means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device that performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, or communication facilities that are connected or related to the device.

(4) "Computer network" means the interconnection of two or more computers or computer systems by satellite, microwave, line, or other communication medium with the capability to transmit information among the computers.

(5) "Computer program" means an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data or perform specific functions.

(6) "Computer security system" means the design, procedures, or other measures that the person responsible for the operation and use of a computer employs to restrict the use of the computer to particular persons or uses or that the owner or licensee of data stored or maintained by a computer in which the owner or licensee is entitled to store or maintain the data employs to restrict access to the data.

(7) "Computer services" means the product of the use of a computer, the information stored in the computer, or the personnel supporting the computer, including computer time, data processing, and storage functions.

(8) "Computer system" means any combination of a computer or computer network with the documentation, computer software, or physical facilities supporting the computer or computer network.

(9) "Computer software" means a set of computer programs, procedures, and associated documentation related to the operation of a computer, computer system, or computer network.

(10) "Computer virus" means an unwanted computer program or other set of instructions inserted into a computer's memory, operating system, or program that is specifically constructed with the ability to replicate itself or to affect the other programs or files in the computer by attaching a copy of the unwanted program or other set of instructions to one or more computer programs or files.

(11) "Data" means a representation of information, knowledge, facts, concepts, or instructions that is being prepared or has been prepared in a formalized manner and is intended to be stored or processed, is being stored or processed, or has been stored or processed in a computer. Data may be embodied in any form, including but not limited to computer printouts, magnetic storage media, laser storage media, and punchcards, or may be stored internally in the memory of the computer.

(12) "Effective consent" includes consent by a person legally authorized to act for the owner. Consent is not effective if:

(A) induced by deception, as defined by Section 31.01, or induced by coercion;

(B) given by a person the actor knows is not legally authorized to act for the owner;

(C) given by a person who by reason of youth, mental disease or defect, or intoxication is known by the actor to be unable to make reasonable property dispositions;

(D) given solely to detect the commission of an offense; or

(E) used for a purpose other than that for which the consent was given.

(13) "Electric utility" has the meaning assigned by Subsection (c), Section 3, Public Utility Regulatory Act (Article 1446c, Vernon's Texas Civil Statutes).

(14) "Harm" includes partial or total alteration, damage, or erasure of stored data, interruption of computer services, introduction of a computer virus, or any other loss, disadvantage, or injury that might reasonably be suffered as a result of the actor's conduct.

(15) "Owner" means a person who:

(A) has title to the property, possession of the property, whether lawful or not, or a greater right to possession of the property than the actor;

(B) has the right to restrict access to the property; or

(C) is the licensee of data or computer software.

(16) "Property" means:

(A) tangible or intangible personal property including a computer, computer system, computer network, computer software, or data; or

(B) the use of a computer, computer system, computer network, computer software, or data.

33.02. Breach of Computer Security

(a) A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.

(b) A person commits an offense if the person intentionally or knowingly gives a password, identifying code, personal identification number, debit card number, bank account number, or other confidential information about a computer security system to another person without the effective consent of the person employing the computer security system to restrict access to a computer, computer network, computer system, or data.

(c) An offense under this section is a Class A misdemeanor unless the actor's intent is to obtain a benefit or defraud or harm another, in which event the offense is:

(1) a state jail felony if the value of the benefit or the amount of the loss or harm is less than $20,000; or

(2) a felony of the third degree if the value of the benefit or the amount of the loss or harm is $20,000 or more.

(d) A person who is subject to prosecution under this section and any other section of this code may be prosecuted under either or both sections.

33.03. Defenses

It is an affirmative defense to prosecution under Section 33.02 that the actor was an officer, employee, or agent of a communications common carrier or electric utility and committed the proscribed act or acts in the course of employment while engaged in an activity that is a necessary incident to the rendition of service or to the protection of the rights or property of the communications common carrier or electric utility.

33.04. Assistance by Attorney General

The attorney general, if requested to do so by a prosecuting attorney, may assist the prosecuting attorney in the investigation or prosecution of an offense under this chapter or of any other offense

involving the use of a computer.

Mike Godwin's Anti-Censorship Speech at CMU

My name is Mike Godwin, and I'm a lawyer with the Electronic Frontier Foundation. My organization, EFF, stands for the proposition that freedom of speech must be protected, not only in the traditional media of speech, print, and broadcasting, but also in the vital new medium of computer communications.

We are not here merely because we are angry, but also because we are grieving over the imminent death of academic freedom at CMU. This fight is not over yet--they still want to review the alt.sex newsgroups and kill the ones they find most embarrassing.

You see, this new medium is ultimately going to become the most important medium for citizens of the United States, and of the world. It is a medium far different from the telephone, which is only a one-to-one medium, ill-suited for reaching large numbers of people. It is a medium far different from the newspaper or TV station, which are one-to- many media, ill-suited for feedback from the audience. For the first time in history, we have a many-to-many medium, in which you don't have to be rich to have access, and in which you don't have to win the approval of an editor or publisher to speak your mind. Usenet and the Internet, as part of this new medium, hold the promise of guaranteeing, for the first time in history, that the First Amendment's protection of freedom of the press means as much to each individual as it does to Time Warner, or to Gannett, or to the New York Times.

Of course, the Supreme Court has long held that, at least in theory, freedom of the press applies as much to "the lonely pamphleteer" as it does to the editors of a major urban daily newspaper. But the Net puts this theory into practice. And it is because the Net holds the promise of being the most democratizing communications medium in the history of the planet that it is vital that we prevent the fearful and the ignorant from attempting to control your access to it.

That's precisely what is happening here at Carnegie-Mellon. There is a strong sense here that, merely because you are students, and because some of you are minors, CMU must protect you from yourselves. They claim that if they don't cut off all access to these newsgroups, for everyone on campus, they'll not only risk perverting you by exposing you to sexually oriented materials, but they'll also be legally liable.

Their claims are wrong. First of all, it's not true that the *only* way to prevent minors from having access to this material is to deny *everyone* access to it. It is clear to me that the administrators haven't explored any alternatives other than the most expensive and infeasible.

Secondly, there is little if any risk of legal liability for the University for carrying these newsgroups, since Usenet is so large that no one can be presumed to have knowledge of all the content of Net traffic, and without proof of that knowledge, says the Supreme Court, there can be no liability. And no university anywhere in the country has ever, at any time, been held liable to any degree for carrying the alt.sex newsgroups.

Third, the risk that the 17-year-olds who enter this University as freshmen are unfamiliar with the materials that are carried in these newsgroups is exceedingly low. Remember, we're talking about high-school graduates here! I submit that if any entering freshmen haven't encountered material that deals with human sexuality before now, CMU has an affirmative duty to expose them to it.

Some members of the University staff have been reluctant to hear these arguments. When I spoke yesterday with attorney Jackie Kastelnik of the University's legal office, she asked me how I got interested in this case. I told her that I had been contacted by several concerned CMU students. At that point she told me that she was not interested in debating me or being informed about the legal issues involved.

But she did say this much to me: "So what if the risk is low! We don't want to be a test case!" To which my response is this: CMU, your lawyers have forgotten the meaning of the Constitution they have sworn to uphold.

Indeed, it's ironic that an institution that focuses so much on memory--of our sciences, our knowledge, our traditions, our values--has displayed so much forgetfulness about the meaning of a University, and has been so inconsistent in deciding what they want you to remember. Remember, before you expressed your concerns, they were ready to kill any newsgroup that dealt with sexual material.

They wanted you to remember the meaning of the Periodic Table, but they wanted you to forget that the chemistry between lovers is one of the most beautiful things we know.

They wanted you to remember the Fundamental Theorem of Calculus, but they hoped you forget that the fundamental fact of human sexuality shapes our entire existence.

They wanted you to remember safety in the lab, but they wanted you to forget alt.sex.safe.

They wanted you to remember the poetry of Dante and Shakespeare and Shelley, but they wanted you to forget that human sexuality, which often inspired these poets, is equally the inspiration of those who write stories and poems for rec.arts.erotica.

It's very clear that this university is all-too- willing to seek a relationship with the Department of Defense, but all-too-unwilling to defend your online discussion of sexual relationships. This is ironic, since this university is ostensibly training you to function as adults in this society, yet it has insisted on treating you like children.

I've talked about what CMU wants you to forget--now let's talk about what they have forgotten.

They've forgotten that the Constitution presumptively protects speech and expression about sexual matters, even when that speech and expression may be offensive.

They've forgotten that the Constitution does not allow governments to ban sexual expression for adults merely because there is some risk that children may see it.

They've forgotten that, when it comes to the Bill of Rights, what you don't use, you lose. The First Amendment is a terrible thing to waste.

As we can see from yesterday's election results, we're living in a conservative era. But the issue at stake here is not one that should divide liberals and conservatives, who have always shared a belief in the importance of individual liberty. In particular, conservatives should insist that CMU not alter its principles in the face of pressure from what may well be a paternalistic government.

But of course it's worth remembering that there has been no such pressure yet. The University has been misleading you as to the risks of carrying this material. And it may be misleading you as to its motives. I strongly suspect that the real reason the Administration tried to yank these newsgroups is that it is embarrassed by them. I spoke with a member of the Administration this morning, and he told me that the University doesn't want to have to defend carrying sexually explicit materials--it's ironic that such a highly educated group is afraid that it won't find the words necessary to defend discourse about a central aspect of the human

condition.

If they lack courage, it's up to you to supply it. Tell the CMU Administration that you came here with the expectation that CMU would live up to the highest principles of academic freedom. Tell them that you expect them to fight as strongly for your freedom of speech and freedom of inquiry as the administrations of Harvard or MIT would.

As Arsenio says, "It's time." Time to remind CMU about the meaning of freedom. And time to tell them once and for all: "No more censorship!"

I urge you not to accept it when the authorities tell you that CMU, as a private institution, is not bound by the First Amendment, and therefore can do anything it likes. This is, of course, quite true, but the issue has never been what CMU is permitted to do--instead, it's been what CMU *should* do if they are to sustain a commitment to academic freedom.

This morning I spoke with a member of the Administration who told me at least twice during our talk that he is a teacher and admirer of James Joyce's ULYSSES--also one of my very favorite books--so he understands the issues raised one someone tries to ban works based on their purported obscenity. When I heard this from him, I felt sad-- how could he possibly have missed the lessons we learned in this society when books like ULYSSES, TROPIC OF CANCER, and LOLITA were litigated in the courts?

It's very easy, I think, to proclaim that you understand the issue of obscenity because you're willing to defend a book that was vindicated half a century ago.

What he doesn't seem to realize is that *this* fight--the one about online freedom of speech--is the one that matters now.
