==Phrack Inc.==

Volume Four, Issue Thirty-Seven, File 1 of 14

Issue XXXVII Index

P H R A C K 3 7

March 1, 1992

˜Promoting The Free Exchange Of Information In The New World Disorder˜

WELCOME TO PHRACK VOLUME FOUR!

"I'm too sexy for my Phrack... Imagine that!"

Looking back at Volume III, we observe some historic dates relating to Phrack:

02/24/89 - Phrack 24 released.
01/18/90 - Knight Lightning raided by the U.S. Secret Service because he was editor of Phrack.
01/23/90 - Phiber Optik and Acid Phreak raided by U.S. Secret Service.
02/06/90 - Knight Lightning and The Prophet indicted in Federal District Court in Chicago, Illinois. The Prophet, The Leftist, and The Ur-Vile indicted in Federal District Court in Atlanta, Georgia.
02/15/90 - Knight Lightning enters plea of NOT GUILTY.
03/01/90 - Erik Bloodaxe, The Mentor, and Steve Jackson Games raided by U.S. Secret Service.

- -

Phrack is BACK! Welcome to the first issue of Phrack Volume Four! This issue we feature "Exploring Info-America" by The Omega and White Knight. Other articles of note include TWO articles by Count Zero, Black Kat's latest installment on his VAX/VMS series, and information on VOS by Dr. No-Good! Also, starting this issue, we introduce Pirate's Cove by Rambone. Its a new regular column about the pirate community. Finally, a very special thanks goes out the the newest member of the Phrack Staff, Spirit Walker for the help with assembling this issue.

There is a little surprise in Phrack Loopback. Our old pal THE DICTATOR has been corresponding with Knight Lightning and myself over the nets. Yes, you heard right! Dale Drew, who played a key role in busting people during OPERATION SUN-DEVIL and spying on our friends at SummerCon '88 is back and believe it or not... he wants Phrack! And speaking of Operation Sun-Devil, the federal government convicted their first defendant -- details in Phrack World News (Part 2).

Phrack World News (Part 3) contains everything you need to know about how the Regional Bell Operating Companies feel about our private hobby bulletin boards and next issue we will have information about what YOU can do about it! Also, next issue watch for preliminary details for SummerCon '92!!! Will ESP be there again?

Before the rumor mill starts churning again, I will clarify what is happening with Phrack management. Crimson Death has decided to retire from Phrack and start working on his new UNIX based BBS, CyberWaste! If you are interested in keeping in touch with Crimson Death, you may do so by writing: cdeath@GNU.AI.MIT.EDU for the time being. However, keep an eye out for the CyberWaste hostname; @DEMONSEED.COM!

Well that's it for now. If you are going to the Second Conference on Computers, Freedom, & Privacy (a/k/a CFP-2) in Washington, D.C. (March 18-20, 1992), Knight Lightning and I will see you there!

Sincerely,

Dispater
phracksub@stormking.com

- -

HOW TO SUBSCRIBE TO PHRACK MAGAZINE

The distribution of Phrack is now being performed by the software called Listserv. All individuals on the Phrack Mailing List prior to your receipt of this letter have been deleted from the list.

If you would like to re-subscribe to Phrack Inc. please follow these instructions:

1. Send a piece of electronic mail to "LISTSERV@STORMKING.COM". The mail must be sent from the account where you wish Phrack to be delivered.

2. Leave the "Subject:" field of that letter empty.

3. The first line of your mail message should read:
SUBSCRIBE PHRACK <your name here>

4. DO NOT leave your address in the name field!
(This field is for PHRACK STAFF use only, so please use a full name)

Once you receive the confirmation message, you will then be added to the Phrack Mailing List. If you do not receive this message within 48 hours, send another message. If you STILL do not receive a message, please contact "SERVER@STORMKING.COM".

You will receive future mailings from "PHRACK@STORMKING.COM".

If there are any problems with this procedure, please contact "SERVER@STORMKING.COM" with a detailed message.

You should get a conformation message sent back to you on your subscription.

- -

Phrack FTP Sites -- Here is the short list of some reliable sites. A more extensive list will appear next issue.

Washington University in St. Louis	WUARCHIVE.WUSTL.EDU 128.252.135.4 Location: /doc/policy/pub/cud/Phrack
Electronic Frontier Foundation	EFF.ORG 192.88.144.3 Location: /pub/cud/Phrack
University of Chicago	CHSUN1.SPC.UCHICAGO.EDU 128.135.46.7 Location: /pub/cud/phrack

- -

Table Of Contents

12. PWN/Part 2 by Dispater and Spirit Walker 30K
13. PWN/Part 3 by Dispater and Spirit Walker 29K
14. PWN/Part 4 by Dispater and Spirit Walker 31K

Total = 346K

One last thing... Ninja Master, this one’s for you!

"But you see you are not anybody. You are nobody.
And you chose to be so of your own free will.
Legally -- officially -- you simply don’t exist!"

From "The Shockwave Rider"

[-=:< Phrack Loopback >:=-]

By Phrack Staff

Phrack Loopback is a forum for you, the reader, to ask questions, air problems, and talk about what ever topic you would like to discuss. This is also the place Phrack Staff will make suggestions to you by reviewing various items of note; magazines, software, catalogs, hardware, etc.

Review of 2600 Magazine Autumn 1991

PO Box 752
Middle Island, NY 11953
InterNet: 2600@well.sf.ca.us
Phone: 516-751-2600
Fax: 516-751-2608

Individual Subscription Rates:
US : 4 issues (1 year) $21.00
OS : 4 issues (1 year) $30.00
Corporate / Business Rates:
: 4 issues (1 year) $50.00

By Dispater

2600 Magazine has been published since 1984 by Emmanuel Goldstein. "The Hacker Quarterly" runs just shy of 50 pages and is printed with nice glossy covers to make a 5.5"x8.25" magazine. In 2600 you will find the usual articles about hacking and phreaking, as well as a few surprises. 2600 often covers topics that do not necessarily pertain to hacking or phreaking, but are quite useful. There is also a "letters to the editor" section and even a place for people to buy/sell goodies.

This particular issue contains an article on Simplex locks and how easy it is to open them. Included are pictures of opened Federal Express mail boxes that use Simplex locks. The next most interesting thing I found was an article on those strange little lines on business letters. "Postal Hacking" will not necessarily tell you how to mail letters for free, but will tell you how you can speed up the process of delivery for free. Then there was the the "Protecting Your Social Security Number" article that was recently printed in Phrack Inc Issue 35.

There was also an article about the video tape of the Dutch hackers breaking into the military systems. 2600 even offers to sell the videotape that was partially played on the evil Geraldo Show [dick]. There was also a good article written about psychology in the hacker world. The somewhat Freudian analysis of the female security agent fearing "mounting" (of her hard drive), "penetration" (of her system), "infection" (from viri), and "has a headache" (due to hackers) was insiteful as well as very funny. Moving on to the other parts of 2600, you can find scattered tidbits of misc information (ie: lists of COCOTs, NUAs, ANIs, small useful programs, and interesting business/government forms they get from readers, etc)

Finally, this is the part that everyone complains about, the price. But, 2600 has a great deal for those poor college hacker out there. If you submit something to 2600 Magazine that is printed, you get a free subscription. That sounds fair to me! Maybe we should try the same thing with Phrack?

All in all 2600 Magazine is a GREAT publication and is highly recommended.

What's On Your Mind?

:: Some People Never Get The Hint ::

Recently Phrack Inc. received a subscription request from an individual who played a key role in Operation Sun-Devil. You may know him from bulletin boards where he often used names like "The Dictator" or "Blind Faith." We know him as Dale Drew. Who would imagine that he would dare to ask us for a subscription? I personally couldn't believe it.

Just in case you forgot or have been living in a hole for the past two

years, Dale Drew was a paid United States Service informant who secretly enabled government agents to videotape SummerCon '88 in St. Louis, Missouri.

The following is an example of a Dale Drew/The Dictator/Blind Faith posting on a bulletin board. He claims to be a cosysop on Lutzifer as well as some other nonsense.

- -

ZDDDDD Packet Switching Networks/PSNs DDDD September 27, 1991 at 8:52 pm DDDDD?
3 Left by Blind Faith (Level 40)Title: Telenet (No Replies)3
3 > <-702-> CoSys on Lutz (Tymnet) <To: Anyone3
@DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDY

Couple of Things:

Anyone, besides myself, have any experience with Tymnets and/or Telenet debuggers? (Xray, TDT2, Isis, etc)... TDT2 on Telenet is great, cus on the private nets they've got a hard-coded password...always gets you in. They used to have it on the public net too, but about two years ago they fixed it. (maybe nbot all of it, but I cant find any that still do)

sprint is a tymnet nui that goes to telenet

telenet is changing there host format. they are adding an extra digit (too many hosts, i guess). so be on the look out for that. Im not sure when, but the customer service rep, was VERY helpful..

--BF
"What, me worry?"
[Message menu] Command (?/Help):

- -

Dale Drew is currently working for Tymnet security. For more information about the activities of Dale Drew, it is highly recommended that you read Computer Underground Digest (CUD) Issue 3.02.

Since I knew that Knight Lightning would enjoy (smirk) hearing from his old pal, I forwarded the mail appropriately to Knight Lightning's email address.

- -

From: ddrew@btnagns.Tymnet.COM (Dale Drew)
To: phrack@stormking.com

I would like to have my name added to the Phrack Mailing List. In the past, I have been getting the Phracks from the University of Chicago, but it would be more convenient to have the Phracks mailed to me.

Also, I was terribly disappointed to see that Phrack had decided to lower its standards of information by releasing the contents of Phrack issue #36.

Dale Drew
Sr. Information Security Specialist

- -

From: Knight Lightning
To: Dale Drew

Dale (DicKtator/Blind Faith) -- I have to admit that you have balls to send a letter to my friends at Phrack and requesting a subscription.

You are a paid informant for the Secret Service. You set people up to get busted. You take people's trust and turn on them. You are a liar and a fraud. You know, Dale, I never imagined such things until a couple of weeks before I

went to trial and I had the opportunity to watch those video tapes of SummerCon '88. You and your fascist Secret Service law enforcement friends definitely put one over on us (even if there isn't anything illegal taking place on those tapes... Great way to spend the taxpayers' money).

So when you wrote to Phrack the other day, did you really think they would not know who you were? Did you expect a warm welcome?

During the time that I was editor of Phrack, I had a policy of inviting law enforcement and security people on to the Phrack mailing list. I don't run Phrack anymore, but my recommendation to the current editors is very simple. They should not send Phrack to you... not because you are with law enforcement... because you are the LOWEST FORM OF LIFE and deserve nothing except our strong dislike.

In short -- I speak on behalf of the modem community in general, "FUCK OFF GEEK!" Crawl back under the rock from whence you came and go straight to hell!

Knight Lightning

- -

From: Dale Drew
To: Knight Lightning

Craig,

Apparently you are not as mature as I was led to believe. Not being on the Phrack mailing list is not a concern to me, it was merely a convenience. Phrack, as I am sure you are aware of, is available all over the net and I will just continue to receive my copies from there.

I had no idea that you and the newly founded editors of Phrack have decided to become so childish. But I suppose things will never change, and that I am sad to see.

--Dale

:: Best Evidence ::

From: John Higdon
To: Dispater

> Dispater writes:
>
> I think the joke issue of Phrack (36) will contain a top 10 list of stupid
> things the SS likes to take.

I am consulting with the defense for an up coming trial and had the opportunity to examine the "evidence" seized in the defendant's home. Notable items: model rocket launcher, local area street maps, about a dozen 2500-style telephones, a typewriter, pre-recorded audio cassettes. An interesting item was left behind: a TSPS console.

One wonders what (if anything) goes through the minds of the officers executing the warrant.

John

:: Fed Proof Your BBS, NOT! ::

I'm sure many of you have seen text files on making your BBS more secure. One such file floating around is by Babbs Boy of Midnight Society. One of the members of our Phrack Staff showed this document to EFF's Mike Godwin, who is an attorney. He had the following comments:

- -

From: Mike Godwin
To: Phrack Inc.

(In regards to some of the files about how to "fed-proof" your bbs:)

> Let's start with the log on screen: If FEDZ want anything from your board,
> they are required to provide 100% accurate information.

This is false. Ask the legislators who've been convicted in "sting" operations. In fact, so far as I can tell in a brief run-through of this document, absolute no part of the so-called "legal" advice is true.

Law enforcement agents who misrepresent their identities (e.g., "undercover agents") produce admissible evidence all the time.

--Mike

:: Diet Phrack is Good For You ::

From: Gordon Meyer
To: Dispater
Subject: Phrack #36

Thanks for sending over Diet Phrack! It looks like some of the old energy has finally been renewed. I especially liked the introduction, there is intensity, pride, and humor sprinkled thru out. Reminds me a lot of some of the "old" PHRACK issues. Neat!

Later,
Gordon R. Meyer

:: Anonymous Mail ::

From: Creeping Death

> Hi guys. I was wondering if you could tell me how to send anonymous
> mail. I heard that you could but no one here at my university seems to have
> a clue. Please help me out
>

There are many ways to do this. One way is to use the method described below. However, keep in mind there are other ways of doing this.

Dispater

- -

Anonymous Mail via SMTP Using A Simple Shell Script
~~~~~~

From: The Artful Dodger

This file is for those people who like/want to send anonymous mail via the net but don't like the hassle of raw SMTP commands. So, I wrote a simple shell script to take care of this. This program is quite simple but I will give a brief explanation anyway.

There are two ways to run this program. Just type the name you save it as or the name you save it as plus the person you want to mail. Either way you will eventually get to the From: prompt. If you just hit return at this prompt it will assign your userid@your hostname. Otherwise you can type whatever you feel like.

Next you will get the prompt asking you which host you wish to use for
~~~~~~

SMTP. If you are using the host you are on, just hit return as this is the default. Otherwise enter any host that allows telnet to port 25. Then you get to pick which editor you wish to use for mailing. It defaults to vi but you can use whatever you like. Basically, that is all there is interactively. After you enter this information, the program creates a file called tmpamail1. To this file it appends four lines of data. The first line is 'helo amail' as some host's SMTP port will not accept commands until one introduces themself to the host. The next line is 'mail from: ' and who the mail is from or who it is supposedly from. The third line contains 'rcpt to: ' and who the mail is going to. And the last line is simply the word 'data'.

Now, these commands could all be entered manually but why bother when you have a program to do it for you. Ok, now the program invokes your editor and creates a file called tmpamail2. After you are done making the message and you exit the editor, it asks you if you want to send this message. I believe that is pretty much self explanatory. Then the program appends a '.' and a 'quit' to tmpamail2. Then it appends tmpamail2 to tmpamail1 so you have one file containing all the necessary header info to send a message via SMTP and quit >from SMTP. Then the program sends all this to port 25 of the host that was specified. And if all goes well, the person should have some mail waiting for them. And one last thing. The program deletes both tmpamail files after it is finished. Well, I hope you all enjoy this little script as it makes sending anonymous mail a little easier.

The Artful Dodger

==========

```
#! /bin/csh -fB
### This is a simple shell script for easy use of anonymous mail.  To run the
### program just save it and delete everything up until the #! /bin/csh -fB
### line.  Then just type the name you save it as or the name and whoever
### you will be mailing.  e.g.  amail bill@some.university.edu or just amail.
###
###   The Artful Dodger

if ($1 != "") then
   set mto=$1
else
   echo 'To: '
   set mto=$<
endif

echo -n 'From: '
set mfrom=$<

echo -n 'Use which host for smtp (return for '`hostname`') ? '
set usehost=$<

echo -n 'Use which editor (return for vi)? '
set editor=$<
if($editor =="") then
   set editor=vi
endif

if ($mfrom == "") then
   set mfrom=`whoami`'@'`hostname`
endif

echo 'helo amail' >> tmpamail1
echo 'mail from: '$mfrom >> tmpamail1
echo 'rcpt to: '$mto >> tmpamail1
echo 'data' >> tmpamail1

$editor tmpamail2

clear
echo -n 'Are you sure you want to send this? '
```

```
set yorn=$<
if($yorn == 'y') then
   echo . >> tmpamail2
   echo quit >> tmpamail2
   cat tmpamail2 >> tmpamail1
   telnet $usehost  25 < tmpamail1 > /dev/null
   echo 'Mail has been sent to: '$mto
   echo '                 From: '$mfrom
endif
rm tmpamail1 tmpamail2
```

Pirates' Cove
Issue One

A New Regular Column Appearing In Phrack Magazine
By Rambone

1) Introduction

Well first off, I'd like to introduce myself. I go by the handle Rambone, and I run a board in the Midwest area. I'm sure a column like this is a shock to a lot of reader's, but after talking to Dispater, many readers, and people in the hacking and pirate world, we came to this conclusion: Piracy and *Warez Dudez* have come a long way in the last five years, and are a definite part of the underground. Whether you read the magazine for information about hacking, phreaking, or even those great PWN stories, I think this column will be a welcome part of Phrack Magazine.

2) Virii

Some poor unsuspecting fool downloads a program, unzips it, and instead of checking it for a virus, starts the program up. After deciding it's a lame game, he deletes it and turns off his computer, going to sleep without a worry in the world. The next day he wakes up and tries to turn on his computer, but it tells him, "Bad or missing COMMAND.COM" or something of that nature.

This is just an example of what's happened to countless people in the pirate world, not expecting what is soon to be hours of frustrating reconstruction of his hard drive. Even though virii have been a common problem for many years, it hasn't been until recently that they have made an impact in the Pirate world.

Whether it's bickering between groups, or even a lonely individual who has absolutely nothing better to do than beat his meat and put out a trainer with a fucking virus in it, it is wrong. The people responsible for it that play a roll in the distribution of the software are, in my opinion, the biggest culprits; they know what they are about to do, and have no conscience in sending it out. Just the mere fact that the only way they think they can get back at another group is by distributing a program with a virus or a Trojan is moronic.

I'm not preaching the fact that groups should or should not bicker. That is always going to happen. What I an saying is that there is a responsibility by the groups to be cool and stop the distribution of programs with virii or Trojan's. On the flip side of the coin, most sysops do not intentionally send out these infected programs. They are sent up to the BBS, and by the time they are caught, it's too late, and they are already all over the country.

My main concern is for the user. If all one group was doing was giving another group problems, then there wouldn't be one. But to irresponsibly release a program containing a virus has to be one of the lowest retaliatory responses that can be done in the pirate world, and needs to be stopped to bring piracy back to a higher level it once had before the rash of bombs began.

Note to user

Most virii are in the form of trainers and cracks, so be wary of every one you have or get. The best way to check is with PKUNZIP -T and McAffee's Virus Scanner; I've found it to be the most reliable. If anyone is having trouble with being able to temporarily open a .ZIP, .ARJ, etc., I have a sharp .BAT file to do this and will type it up in a future issue. DO NOT use a program without at least scanning the directory you unzipped it to, even though scanning the zip is much safer.

3) Nets

Some issues here will be the discussion of up and coming nets, as well as established ones. Let me first explain what a net is: a net is a group of messages sent out over the networks via modem. They are then received by a BBS and sent to the appropriate message subs for the sysop and users to read. One up and coming net in particular that would be appealing to a wide variety of sysops is called "CyberCrime." This net is looking for boards that are Fido compatible, i.e.: LSD, Telegard, WildCat, Tag, Remote Access, Omega, QBBS, Paragon, Infinity, Revelation, Cypher, etc. This net is heavy into P/H/C/A as well as pirate discussions. They are also hooked into TSAN general discussions and are working on sysop's connections with other nets. If you are interested in joining this net, apply at Infinite DarkNess, (305)LOOK4-IT, log on as Cybercrime and password=Death, and follow the instructions. Fill out the CyberCrime node application. MidNight Sorrow will call your BBS (must be a full-time system), login, and upload CYBER.ARJ, the CyberCrime official start-up kit. After that, you're in.

4) BBSes

Because of NSHB/USA/TGR busts, I have decided to hold off on any reviews of BBS's. Hopefully the paranoia over these busts will subside, and we can pick this area back up.

5) News Update

Well, as we all know by now, The NotSoHumble Babe and The Grim Reaper, sysop of The Void, got busted for carding. This has been written up and talked about in every magazine out, so all I'm going to say is that it's brought a lot of paranoia to the pirate community, and some good boards have gone down as a result. Since I have not spoken to Amy or Mike about this I will not go into specifics. Amy (NSHB) was a member of USA (United Software Association) and Mike (TGR) ran a BBS called The Void, and was an INC Distro Site. But until I hear back from a certain person at USA, I'm not going to talk about some 3rd party gossip, so this will be continued in the next issue.

6) New Warez

Game of the Month:

Star Trek: 25th Anniversary

Graphics	[CGA/EGA/VGA]
Sound	[ADL/SNB/PCSPK]
Controls	[Mouse/JS/KYB]
Cracked by	[EMC/USA/Razor?]
Supplied by	[?]
Cracked by	[Separate Crack]
Protection	[Dox Check]

Three cracking groups claimed to put this out first. Since I saw it released by EMC first for a few hours, this is who I'll go with. This is one of those games that, whether you are a Trekkie fan or not, you'll love. The opening screen depicts the Enterprise screaming across your screen, and the music from the original soundtrack blares through your speakers (if you use a soundcard). You then are thrust into a mock battle with another ship, and your adventure begins. You are then directed by Star Fleet to go on your first mission, where you will try and save a planet. The graphics are excellent, and remind me a lot of the new Sierra-type games, with the backgrounds painted in. This game has an adventure theme as well as several space combat scenarios, and a mouse is recommended to be able to get around as quickly as you can in combat scenes. The puzzles involved are very hard, and there is both a walk-through and cheat out on your local BBSes. So if you cannot get through some of the puzzles, there is help out there; you just have to find it.

Note

Well that’s it for now. I had to take out 60% of this article because many people are laying low for a couple of months, so look for more in-depth coverage in the future including interviews, BBS reviews, profiles, and cracking tips.

```
:===:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:===:
:==                                                                      ==:
:==                    Exploring Information-America                     ==:
:==                   :==============================:                   ==:
:==                                 by                                   ==:
:==              The Omega                         White Knight          ==:
:==  Restricted Data Transmissions (RDT)      Cult of the Dead Cow (-cDc-)  ==:
:==                                                                      ==:
:==                                                                      ==:
:==                 "Truth Is Cheap, But Information Costs!"             ==:
:==                                                                      ==:
:==                        ------------------------                      ==:
:==                                                                      ==:
:==        "Textfiles:  We're in it for the girlies and the money."      ==:
:==                                                                      ==:
:==  Monkey-Boyz!                                                1/24/92  ==:
:===:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:=:===:
```

Introduction

The Information Era has only recently come of age; powerful database technology has become more affordable to implement (witness MCI's ability to maintain a database of the people you most frequently call for participation in its Friends & Family program), and parallel to it, information gathering has become more extensive and more scrutinizing. After weapons manufacturing, and drug running, "information gathering" is probably one of the most profitable enterprises in America.

Over the past two decades, credit bureaus, telephone companies and direct marketers have collectively amassed complete consumer profiles on over 150 million Americans. But for the most part, this information has been used only to predict consumers' future buying habits, or worse: to influence them. For billing and marketing purposes, up-to-date address and telephone information, as well as information about your household has been incidentally maintained.

But, until recently, none of this information was COMMERCIALLY available IN A SINGLE DATABASE, specifically with law enforcement, private-investigators, bounty-hunters and lawyers in mind. To our knowledge, Information America is the first accessible service to make use of previously collected data for the expressed purpose of providing the up-to-date whereabouts, personal profiles and information regarding legal entanglements (i.e., bankruptcy filings, lawsuits, etc.) of as many Americans as possible.

Information America

> "Whether you are conducting a background check, looking for a witness, skip tracing, or gathering information for court, [Info America] gives you a quick, easy method for gathering information on individuals across the country... at the touch of a key."

Information America (IA) provides a single service whose databases cross-index the Postal Service's National Change of Address file (NCOA), major publisher and direct marketing companies' client information, birth records, driver's license records, phone books, voter registrations, various governmental records, and more. IA boasts that over 111 million names, 80 million households and 61 million telephone numbers are maintained (as reasonably up-to-date as possible) on-line.

Together with IA's access to additional databases, such as Dun & Bradstreet, Secretary of State records and records from up to 49 government agencies, you can:

* Locate a missing defendant or witness and obtain a neighbor listing for further investigation.

* Locate corporate officers, share-holders, or missing heirs.

* Locate individuals for collection purposes.

* Locate a fugitive parent who's kidnapped his child from the other parent during a custody battle.

* Identify the corporate affiliations of an individual.

* Examine bankruptcy, lawsuit, liens and judgement records on individuals and businesses.

* Examine Securities and Exchange Commission filings and business news compiled from major newswires.

* Gather information about a company's officers, ownership, financial status and parent/subsidiary relationships.

* Determine if a foreign corporation has a resident agent for local service of process (i.e., for serving a lawsuit).

Logging onto IA

Access to Information America is provided through your local Tymnet dialup (7-E-1); use a terminal identifier of 'a', and type "infoam" at the "please log in:" prompt. IA will prompt you with the familiar VAX 'USERNAME' and 'PASSWORD' prompts. Usernames of the form "BIDAxxxx" (where x is a digit) are recognizable to the VAX as IA accounts and cause it to execute the script that provides the interactive database environment once the correct password is supplied. Accounts which bypass the interactive environment and provide you with the normal VAX shell-access must exist, but neither White Knight nor I have explored that avenue.

In any event, once you log on, you are greeted with something similar to:

```
----------------------------[ Title Screen ]----------------------------

    Welcome to VAX/VMS version V5.4-2 on node ALAMO
 Last interactive login on Thursday, 17-SEP-1991 12:47


                COMPUTER EQUIPMENT SELECTION MENU


  What type of computer equipment or software are you using?


      1.  PERSONAL COMPUTER (or 100% IBM compatible)
      2.  PERSONAL COMPUTER with WESTMATE SOFTWARE
      3.  WESTLAW TERMINAL
      4.  OTHER EQUIPMENT
      5.  NETWORK SYSTEM (TTY)

     99.  EXIT OFF SYSTEM


  Please call Information America's Client Support at 1-(800) 235-4008
  if you would like assistance.


Please specify number: 1

  * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
  *                                                                     *
  *               W E L C O M E   T O   T H E                           *
  *                                                                     *
  *     I N F O R M A T I O N   A M E R I C A   N E T W O R K           *
  *                                                                     *
```

* *

For details select menu option 75 on the beginning IA Menu

* Information America Expands California Lawsuits!

* Global Real Property Asset Locator Now Online!

* Cover All the Bases...Using the NEW, IMPROVED CORPORATE GLOBAL Service!

Enter your name (last name first): public, john

----------[Title Screen]----------

In most cases, IA's clients use IBMs or compatibles to connect. However, option 1 (PERSONAL COMPUTER (or 100% IBM compatible)) works well enough for anyone who can emulate VT-100.

The "Enter your name (last name first)" prompt is purely for your own internal billing purposes so that you, as a legitimate account holder, can track account use by separate members of your corporation. Hypothetically speaking, if someone were interested in accessing the system without a valid account of their own, the most likely way to alleviate suspicion would be to use the name of someone who actually works at the account holder's organization -- the account holder himself, for instance.

At some point, IA will prompt you to enter a Client Billing Code. Again, this information is purely for the account holder's own internal billing purposes. IA is an expensive service; on top of the $95 per month fee, there are hourly connect charges, per-item charges and several hidden costs. If only for that reason alone, IA's clients tend to be very anal about cross-checking their itemized bills. If possible, provide a Client Billing Code which is consistent with the account holder's organization's billing code scheme.

Information America: Main Menu

There are 19 main search-options available through IA, which fall into three categories:

- Corporate, UCC, & Related Records
- Nationwide Services
- County & Court Records

----------[Main Menu]----------

INFORMATION AMERICA NETWORK 1

I N F O R M A T I O N A M E R I C A B E G I N N I N G M E N U
(Copyright 1991, Information America, Inc.)

CORPORATE, UCC, & RELATED RECORDS
1. Corporate Global (CGL)
2. Corporate & Limited Partnership Records (COR)
3. State & County UCCs, Liens & Judgments (ULJ)
4. State UCC & Lien Filings (UCC)

5. Sleuth (SL)
6. Litigation Prep (LP)

NATIONWIDE SERVICES
7. People Finder (PF)
8. Executive Affiliation (EA)
9. Business Finder (BF)
10. Business News (BN)
11. SEC Filings (SEC)
12. Duns Business Records Plus (DB)
13. Name Availability/Reservation (NAR)

COUNTY & COURT RECORDS
15. County Records (COU)
16. Bankruptcy Records (BNK)
17. Lawsuits (LS)
18. Real Property Asset Locator (RP)
19. Real Prop, Liens & Judgments (RLJ)

75. Help Line (HL)

14. Document Ordering eXpress (DOX) 99. Exit the System (OFF)

Enter the menu number or abbreviation of your choice:

----------[Main Menu]----------

Of the three categories, options under NATIONWIDE SERVICES are the most interesting. Information America is easy to use, completely menu-driven and features extensive on-line Help. That having been said, White Knight and I will cover only a few of IA's features and leave exploration of the more obscure ones to the reader.

PEOPLE FINDER

The power of People Finder lies not only in its ability to tap various large store-houses of data, but in its flexibility of search criteria. (NOTE: People Finder is available Monday through Friday, 7:00 AM to midnight, Eastern Standard time. Holidays are excluded.)

People Finder is made up of four services: SKIP TRACER, TELEPHONE TRACKER, PERSON LOCATOR, and PEOPLE FINDER MULTITRACK.

Depending on the information available, a People Finder profile may include current address, telephone number, residence type, length of residence, gender, date of birth, up to four household members and their dates of birth and a neighbor listing.

SKIP TRACER traces a person's moves or verifies the current address when all you have is an old address. You will enter the person's name, street number, street name, and either the Zip Code or city/state. If your subject is in IA's files, a profile will display that includes the address he moved to (or current address), phone number, length of residence, and more. You may also request a list of 10 of the person's neighbors. A profile on the current resident at your subject's old address and up to 10 neighbors there may also be available. This gives you several contacts to help you find your subject.

TELEPHONE TRACKER tracks down the owner of a telephone number. You must enter the phone number and either the area code or the city/state. If a match is found, you may look at a profile of that individual/residence and a listing of up to 10 neighbors.

PERSON LOCATOR helps you locate a person when specific address information is unavailable. Enter the person's name and indicate whether you wish to conduct a search by city, state(s), zip or nationwide* PERSON LOCATOR will compile a list of names (up to 300 names for nationwide and up to 100 names for individual state searches) that match the information entered. When you find the right name, you may request a profile and neighbor listing for that individual.

PEOPLE FINDER MULTITRACK helps you locate multiple people during one search. Search results are available the following business day. For each of your subjects, enter the name and indicate the geographic area you wish to search -- nationwide*, multi state, state, city or zip. You may enter up to 25 names per search. Sign off the system and let Information America do the work for you. The following business day, log on to Information America and access the People Finder Menu by entering PF at the Information America Beginning Menu. From the People Finder Menu, you may view the results of People Finder MultiTrack by entering RR (Review People Finder MultiTrack).

REVIEW PEOPLE FINDER MULTITRACK allows you to review the status of each of the searches you requested. You may choose to view the results of each completed search at this time. Search results will be stored for seven days from the day you requested the search. You may review the search results at any time during the seven-day time period through the Review People Finder MultiTrack option. Search results include a summary listing of names that match the information entered (up to 300 names for nationwide and up to 100 names for individual state searches). From the summary, you may select individual profiles and

neighbor listings.

* Nationwide search is not available for specific common surnames. For a list of these surnames, enter #92 View Common Names (VC), from the People Finder Menu.

```
   -------------------------[ People Finder Menu ]-------------------------

INFORMATION AMERICA NETWORK

                        P E O P L E    F I N D E R
                 (Copyright 1991, Information America, Inc.)
            Client Billing Code: 123456

    1. Person Locator (PL)           (Search by name & location)
    2. Skip Tracer (ST)              (Search by name & last known address)
    3. Telephone Tracker (TT)        (Search by telephone number)
    4. People Finder MultiTrack (PX) (Multiple searches by name & location
                                      with results available next business day)
    5. Review People Finder MultiTrack Results (RR)

                   70. Revise Client Billing Code  (BC)
                   75. Help Screen  (?)
                   92. View Common Names (VC)
                   95. Description of Service  (DES)
                   99. Go to Beginning Menu  (BEG)
                   OFF Exit off the System  (OFF)

   -------------------------[ People Finder Menu ]-------------------------
```

If People Finder locates your subject, a profile containing the following information can be displayed:

Name	Usually first and last name of head of household.
Address	Street or route, city, state, and ZIP.

* The following fields will display only if the information is available. *

Phone Number	Current phone number, if listed in the phone book.
Approx. Birth Date	Birth date of the individual listed in the Name field. (May be an approximation.)
Gender	(FEMALE, MALE, UNKNOWN) Refers to person in Name field.
Length of Residence	Number of consecutive years this person has appeared at this address.
Residence Type	Number of last names found at this address. (Useful in identifying multi-family residences.) Can be single, double, triple, quad, 5-9 units, 10-19 units, 20-49 units, 50-100 units, 100+ units.
Additional Household Members	Names and approximate birth dates of up to 4 individuals residing at this address and having the same last name as person listed in Name field. (Usually taken from birth records.)

People Finder: A Sample Search

```
   ----------------------[ People Finder Search ]----------------------

Last Name:   public                    First Name:   jane
Enter City or ZIP code.
City: ANYTOWN                          ZIP Code: 90210


Searching...
```

Name Searched: PUBLIC JANE

PERSON LOCATOR
Last Name Summary

No.	First Name	Street	City/State	ZIP	Phone No.
1	JANE	27 AVENIDA AVE	ANYTOWN	CA 90210	213-727-8023
* 2	JOHN	69 CALLE DE LOS PUTOS	ANYTOWN	CA 90211	213-000-0000

* PUBLIC JANE has been found as an additional household member.

Searching...

INFORMATION AMERICA NETWORK--PEOPLE FINDER - Detail
Name Searched: PUBLIC JANE

PERSON LOCATOR
Resident Profile

Name: JANE PUBLIC
Address: 27 AVENIDA AVE
ANYTOWN, CA 90210
Approximate Date of Birth: 10/66
Gender: FEMALE
Length of Residence: 3 YEARS
Residence Type: SINGLE

**** Additional Household Names ****

Name	Approximate Date of Birth
MICHAEL	04/68

Searching...

INFORMATION AMERICA NETWORK--PEOPLE FINDER - Detail
Name Searched: PUBLIC JANE

PERSON LOCATOR
Neighbor Listing

Resident: JANE PUBLIC
Address: 27 AVENIDA AVE
ANYTOWN, CA 90210

Name	Phone#	Address	Residence Length(yrs)/Type
WILLIAM PRESTON	(818) 727-8125	12 BOGUS AVE	12 SINGLE
THEODORE LOGAN	(818) 725-8643	17 BOGUS AVE	04 DOUBLE
KRIS APPLEGATE	(818) 685-2112	19 BOGUS AVE	03 TRIPLE
MARTIN MCFLY	(818) 727-0353	26 BOGUS AVE	23 SINGLE
STAN CISNEROS	(818) 727-4973	30 BOGUS AVE	16 SINGLE
LUCY BYRNE	(818) 727-8765	33 BOGUS AVE	10 SINGLE
JONATHAN DEPP	(818) 725-2012	35 BOGUS AVE	06 SINGLE

----------[People Finder Search]----------

Notes on People Finder

IA is only as accurate as public records reflect. People who move frequently or move from apartment to apartment (students, for instance) are either not likely to be found in IA, or the information IA provides is likely to be out-dated. In one search we performed, IA concluded that our subject had lived at his residence for 3 years when, in fact, the subject had been living there for over 15 years.

Unlisted telephone numbers are frequently available through IA if, for example, your subject's unlisted number has appeared in a City Directory. Curiously, information seems to be disappearing from IA, in some cases. A year ago, White Knight and I looked up a celebrity's address and telephone number, both of which IA correctly found. When we performed the same search recently, IA failed to find the celebrity in its records. Searches on other individuals which once listed their unlisted telephone numbers now yield "000-0000". We have no explanation for why this seems to have happened.

Overview of IA's other options

SLEUTH

By creating a list of affiliated names -- "clues" -- Sleuth helps you uncover relationships between businesses and individuals. Enter a name and check official records from up to 49 government agencies.

CONTENTS: Over 100 searches* combined in one... from these services:

State UCC/lien filings in: CA,CO,IL,IA,MD,MA,MO,NE,NC,PA,SC,TX
Corp/LP records in above states, PLUS: AZ,CT,DE,GA,IN,MI,NV,OK,OR,UT,WI
Sales and Use Tax information in: CA, TX

County Assumed/Fictitious Names from: Los Angeles, San Francisco (CA)
Dallas, Harris (TX)
County UCC filings from: Fulton, Cobb, DeKalb, Gwinnett (GA)
Dallas, Harris (TX)

LITIGATION PREP

CONTENTS: State Corporate & Limited Partnership Information from:
Arizona*, California, Colorado, Connecticut*, Delaware, Florida, Georgia, Illinois*, Indiana, Iowa, Maryland, Massachusetts, Michigan, Missouri, Nebraska, Nevada, North Carolina*, Oklahoma, Oregon, Pennsylvania, South Carolina, Texas, Utah, Washington, and Wisconsin (* indicates Limited Partnership information is not available from these states).

Searches include the following, where available:
Business Names, Owner Names, Prior Names, Assumed Names, Fictitious Owner Names, Trade Names, DBA Names, and Merged Out/Consolidated Names

GENERAL DESCRIPTION: Litigation Prep allows you to simultaneously search state corporate and limited partnership information and county-filed fictitious business and assumed names, to assist you in obtaining the details you need to begin preparing a lawsuit.

HOW THIS SERVICE WILL HELP YOU: Litigation Prep is designed to help litigation professionals when gathering information to file a lawsuit. This service provides the researcher with valuable pieces of information, such as business name, agent name and address, principal address, type and status. Good Standing/Existence Status is also available in the following states:

AZ, CT, DE, GA, IL, IN, IA, MA, MI, MO, NE, NC, OK, OR, PA, SC, TX, UT, WA, and WI.

CONTENTS/SOURCES: Below, you will find the informational contents searched in each state. Inactive records are included for informational purposes. Unless otherwise specified, files are updated weekly.

HOURS: Litigation Prep is available Monday through Friday, from 8:00 AM to 12:00 AM Eastern Time. The FLORIDA component of the service is only available >from 8:30 AM to 7:00 PM Eastern Time, Monday through Friday.

CORPORATE GLOBAL, CORPORATE & LIMITED PARTNERSHIPS
========= ====== ========= = ======= ============

CONTENTS: State Corporate & Limited Partnership Records from:

AZ*, CA, CO, CT*, DE, FL, GA, IL*, IN, IA, MD, MA, MI, MO, NE, NV, NC*, OK, OR, PA, SC, TX, UT, WA, and WI
(* indicates Limited Partnership Records are not available from these states).

States included in the Officer/Partner Name search:

CA, CO, FL, GA, IL, IN, IA, MA, MI, MO, NV, OR, PA, TX, and UT.

State Corporate and Limited Partnership Records are available in many key states. A complete listing of states and the information provided by state is available on the following screens. Records are accessible one state at a time or all at once (CORPORATE GLOBAL). When you conduct a CORPORATE GLOBAL name search, an Index screen will list in which states matches have been found. You can either review all matches, or select specific states to view.

From the CORPORATE GLOBAL menu, you have the following search capabilities:

Business Name - Includes all entities available in the online state corporate & limited partnership files.

Officer/Partner Name - Information varies by state, but may include officers, directors, incorporators and partners.

Note: Individual states offer additional options such as a search by Corporate ID (Charter) Number or Registered Agent Name.

SOURCE & UPDATE INFORMATION:

State Corporate & Limited Partnership files are obtained from the official state agency. Records searched vary from state to state. For the exact types searched by state, see the following screens. Inactive records are included for informational purposes. Files are updated weekly unless noted in each specific state description.

In California and Texas, there is a unique search option called BUSINESS LOCATOR.

In California, this option searches the Board of Equalization (BOE), Licensing and Taxation Information which is the official governing source of California Sales and Use Tax permit holders. This information is available only from the California menu and is not included in the Global service. The file is updated monthly.

In Texas, this option searches the Sales & Use Tax Taxpayer Information file, which is comprised of the official record of the Office of the Comptroller of Public Accounts. As in California, this information is available only from the Texas menu and is not included in the Global service. The file is updated by Information America weekly.

STATE & COUNTY UCCs
===== = ====== ====

CONTENTS: State UCC and lien filings from:
California*, Colorado*, Florida, Illinois, Iowa*, Maryland, Massachusetts*, Missouri, Nebraska*, North Carolina, Pennsylvania, South Carolina, and Texas*.
(* indicates Lien filings available from these states)

County UCC, lien, and judgment filings from:

California: Los Angeles and San Francisco counties
Georgia: Cobb, DeKalb, Fulton, and Gwinnett counties
Texas: Dallas Metroplex and Harris county

GENERAL DESCRIPTION: State & County UCCs, Liens and Judgments allows you to search state UCC and lien filings, plus county UCC, lien and judgment filings.

HOW THIS SERVICE WILL HELP YOU: State & County UCCs, Liens and Judgments may be used by anyone who is looking for information on outstanding UCCs, liens or judgments on an individual or business, as well as assets or financial obligations. For example, litigators, real estate specialists, and merger and acquisition specialists may use this service to assist them in the following ways:

Litigators:
- ** Obtain financial information on prospective clients
- ** Help determine the outstanding obligations of the opposing party which could impact the client's ability to seize assets
- ** Help determine the financial relationships between the opposing party and other entities
- ** Help determine if the debts and obligations of the opposing party are a possible motive for filing suit

Real Estate Specialists:
- ** Conduct a cursory look at the beginning of the transaction to help determine the existence of filings which could cloud title
- ** Help determine if the seller has outstanding tax liens filed against him/her
- ** Help determine whether any personal property involved with the transaction has a prior security interest

Merger and Acquisition Specialists:
- ** Help determine financial standing of a firm or a principal of the firm and identify outstanding obligations
- ** Help determine the financial relationships the firm or principal has with other entities
- ** Determine personal property owned by the firm or principal that is being used to secure loans
- ** Conduct a final check before closing to help confirm that no new matters have been filed which could adversely affect the transaction

SEARCH RESULTS: Searches by Name will retrieve matches of the name searched in the following:

From the state UCC and lien files - debtor names
From the county UCC, lien and judgment files -
California: grantors
Georgia: grantors, taxpayers, debtors, and defendants
Texas: all parties (in Dallas Metroplex); grantors and grantees (from Abstracts of Judgment only), and debtors (in Harris County)

PLEASE NOTE: Searches of debtors in Florida will retrieve only active filings. The option to view Florida's inactive files is offered, at no additional charge, when you select either E (=Exit) or N (=New Search) from the summary screen or last page of a detail report.

HOURS: State & County UCCs, Liens and Judgments is available Monday through Friday, from 8:00 AM to 12:00 AM EST. The FLORIDA component of the service is only available from 8:30 AM to 7:00 PM EST, Monday through Friday.

STATE UCC & LIEN FILINGS

GENERAL DESCRIPTION: STATE UCC & LIEN FILINGS allows you to simultaneously search UCC and lien filings in all of the states that Information America has on-line or you may search filings in a specific state.

Our UCC service includes documents filed under the Uniform Commercial Code in the following states:

California	Colorado	Florida
Illinois	Iowa	Maryland
Massachusetts	Missouri	Nebraska
North Carolina	Pennsylvania	South Carolina
Texas		

Additionally, the following liens are included:

California: Federal and state tax liens, attachment liens and judgment liens.
Colorado: Federal tax liens and judgment liens.
Iowa: Federal tax liens, Verified liens and Thresherman's liens.
Massachusetts: State tax liens and child support liens.
Nebraska: Agricultural input liens, consumer liens, and statutory liens.
Texas: Federal tax liens, utility security instruments, and farm filings.

SOURCE: Data is obtained directly from the official state sources: The Secretary of State in California, Colorado, Illinois, Iowa, Massachusetts, Missouri, Nebraska, North Carolina, South Carolina and Texas; the Department of State in both Florida and Pennsylvania; and the Maryland Department of Assessments and Taxation.

SEARCH RESULTS: Unless indicated otherwise, a debtor name search will reveal listings of active and inactive debtors that match the name being searched. A secured party/assignee search will result in a list of matching active and inactive secured parties and assignees. Instrument numbers can be searched only in an individual state.

In FLORIDA, a debtor or secured party search will reveal only active filings. The option to search Florida's inactive files is offered, at no additional charge, at the end of a detail report for an active Florida UCC.

In MASSACHUSETTS, a secured party search will locate secured parties and, if the UCC has been assigned, assignors; it will not locate assignees since they are not included in the database.

HOURS: STATE UCC & LIEN FILINGS is available Monday through Friday, from 8:00 AM to 12:00 AM EST. The FLORIDA component of the service is only available >from 8:30 AM to 7:00 PM EST, Monday through Friday.

COUNTY COURT RECORDS

Information America provides online access to local court records from four states.

California - Records are available from Los Angeles, Orange and San Francisco counties. Real Property Asset Locator is available for the entire state.

Georgia - The Atlanta metro area is online. It includes Cobb, DeKalb, Fulton, and Gwinnett counties.

Pennsylvania - Records are available for Philadelphia county.

Texas - Records are available for the Dallas/Fort Worth metro area, which includes Collin, Dallas, Denton, and Tarrant counties. Records are also available for Harris County (Houston).

Records vary from county to county, but may include Abstracts of Judgment, Assumed Names, Civil Suits, County UCCs, General Execution Dockets, Limited

Partnerships, Lis Pendens, Probate and Domestic Suits, Real Property Filings, Tax Liens and Trade Name Index. The Court Record menus specify the records available in each county.

LAWSUITS

LAWSUITS EFFECTIVE DATE INFORMATION

File	Source	Begin	Through
CALIFORNIA			
Los Angeles County	County Clerk	01-01-80	12-31-91
Civil (Superior)			
Domestic (Superior)			
Probate (Superior)			
Criminal (Superior)		01-01-80	12-31-91
Orange County	County Clerk	01-01-85	12-13-91
Civil (Superior)			
Family Law (Superior)			
San Mateo County	County Clerk	01-01-84	11-09-91
Civil (Superior)			
CALIFORNIA			
Santa Clara County	County Clerk	01-01-85	12-04-91
Civil (Superior & Municipal)			
Probate (Superior)			
Criminal (Superior)			
Family Law (Superior)			
Contra Costa County	County Clerk	01-02-80	11-30-91
Civil (Superior)			
Probate (Superior)			
Family Law (Superior)			
Wills		01-02-90	11-30-91
San Diego County	County Clerk	06-18-74	01-16-92
Civil (Superior)			
GEORGIA			
Cobb Civil (Superior)	County Clerk	1982	01-17-92
DeKalb Civil (Superior)	County Clerk	1981	01-15-92
Fulton Civil (Superior)	County Clerk	1980	12-26-91
Gwinnett Civil (Sup/State)	County Clerk	1990	01-18-92
ILLINOIS			
Cook Civil Law Division All Districts (Circuit)	Clerk of Circuit Court	01-01-75	12-16-91
Cook Civil Municipal Division 1st District- Chicago- (Circuit)	Clerk of Circuit Court	01-01-85	12-16-91
NEW JERSEY*			
Civil Law Division	Clerk of Superior Court	01-01-88	SEE BELOW

Atlantic	12-09-91	Bergen	11-19-91	Burlington	12-03-91
Camden	11-20-91	Cape May	12-05-91	Cumberland	10-18-91
Essex	12-04-91	Gloucester	12-09-91	Hudson	12-06-91
Hunterdon	12-10-91	Mercer	10-17-91	Middlesex	12-06-91
Monmouth	11-08-91	Morris	12-05-91	Ocean	12-04-91
Passaic	12-04-91	Salem	12-09-91	Somerset	11-22-91
Sussex	11-25-91	Union	12-02-91	Warren	12-02-91

*New Jersey Superior Court Civil Lawsuit information is collected for Information America. Extreme care is exercised in gathering this information. However, it is not the official legal reporting organ of the New Jersey Superior Court. Information pertaining to civil action arising from automobile accident claims, forfeiture, condemnation and name change litigation is not collected and is not contained in this file.

NEW YORK			
New York (Supreme) & Suffolk County (County)	Office of Court Administration	***	01-13-92

*** The beginning dates for New York County's Supreme Civil Court and Suffolk County Civil Court cases vary from county to county and are listed below. The "Current Through" date represents the date the Office of Court Administration last compiled the information for Information America.

Bronx	11-1985	Nassau	02-1978	Queens	12-1985
Dutchess	08-1985	New York	11-1985	Rockland	09-1985
Erie	11-1985	Orange	08-1985	Suffolk	03-1983
Kings	11-1985	Putnam	08-1985	Westchester	01-1981

PENNSYLVANIA			
Philadelphia Civil (Common Pleas)	Office of Prothonotary	01-1982	01-11-92
TEXAS			
Dallas Civil (District)	County District Court	01-01-70	01-10-92

REAL PROPERTY ASSET LOCATOR

Real Property Asset Locator integrates information from several sources to help users identify and estimate the value of real assets or identify the owner of a particular piece of property.

The information, which is collected for Information America, is comprised of the tax assessor's official roll in each county. Additional information is obtained from private source databases to enhance tax roll information.

Real Property Asset Locator provides four ways to search.

1. Asset Locator -- Discover the property owned by an individual or business by entering the name. You may conduct a global, statewide, metro area, county or city (where taxes are assessed at municipal level) search.

2. Ownership Locator -- Discover the identity of the property owner by entering the address of the property in question.

3. Property of Comparable Value -- Estimate value of real property based on sales of similar real property in the given geographic area.

4. Assessor's Parcel Number -- Discover the identity of the property owner by entering the Assessor's Parcel Number of the property in question.

Real Property Asset Locator is available in Arizona, California, Washington DC, Delaware, Florida, Georgia, Illinois, Kansas, Maryland, Massachusetts, Missouri, New Jersey, New York, Pennsylvania, Texas and Virginia.

REAL PROPERTY ASSET TRANSFERS

Real Property Asset Transfers integrates information from several sources to help you identify recent real property ownership transfers.

Use Real Property Asset Transfers to help confirm that your party still owns a particular piece of property or has recently acquired new property.

Real Property Asset Transfers provides two ways to search.

1. Asset Transfers--Discover the property acquired or sold by an individual or business by entering the name. You may conduct a statewide, metro area or

county search.

2. Ownership Transfers--Discover the identity of the seller and buyer of a particular piece of real property by entering the address of the property in question.

Real Property Asset Transfers information, which is collected for Information America, is derived from deed transfers maintained by county recorders' offices in each county. However, it is not the official legal reporting organ of the county recorders' offices.

Real Property Asset Transfers is available in select counties in Arizona, California, Colorado, District of Columbia, Florida, Georgia, Hawaii, Illinois, Maryland, Massachusetts, Nevada, New Jersey, New York, Ohio, Pennsylvania, Tennessee, Virginia, and Washington.

EXECUTIVE AFFILIATION
========= ===========

CONTENTS: Over 30 million executives nationwide. One search will display companies nationwide where an individual is listed as an executive. Two types of reports may be available: the Executive Profile and the Executive Brief.

The Executive Profile is derived from information gathered by American Business Information, Inc (ABI). ABI compiles business listings from the yellow pages of 5,000 telephone directories. Telephone calls to every business are then conducted to collect the executive name and title.

The Executive Brief is derived from Corporate and Limited Partnership Records filed in the following states: AZ,CA,CO,CT,FL, GA,IL,IN,IA,MD,MA,MI,MO,NE,NV,NC,OK,OR,PA,SC,TX,UT,WA,WI. NOTE: Delaware Records are not included.

Executive Affiliation is invaluable when you need to know the business affiliations of an adverse party. When you enter an executive's name, reports on over 30 million executives nationwide are searched. You will receive a Summary Screen with a concise listing of where your selected individual is listed as an executive. The detail report for each affiliation will be either an Executive Brief or an Executive Profile.

The Executive Profile is derived from yellow page listings of 5,000 telephone directories nationwide. The listings are individually verified to collect the name of the top executive at that location and their title. The information report may include this information in addition to the business address, telephone number, SIC code, and type of business. The titles for which an Executive Profile may be available include: President, Vice President, Chairman of the Board, Owner, Executive Director, Manager, Administrator, Principal, Publisher, Pastor, and Rabbi.

The Executive Brief is derived from Corporate and Limited Partnership Records filed in the following states: AZ, CA, CO, CT, FL, GA, IL, IN, IA, MD, MA, MI, MO, NE, NC, NV, OK, OR, PA, SC, TX, UT, WA, & WI.

(NOTE: Delaware Records are not included. Florida Records are available Monday through Friday, 8:30 a.m. to 7:00 p.m. EST.) The second line in the detail heading will list from which state Corporate/LP Record the information is obtained. The information report may include executive name, title, address, business name and address, as well as other executives' names, titles, and addresses associated with that business. Executive Briefs may be available for Officers, Partners, Agents, and Incorporators.

USE EXECUTIVE AFFILIATION TO:

* Learn about an adverse party's business affiliations as part of background checking.

* Verify names and addresses for pleadings and depositions.

* Uncover an executive's involvement in different businesses throughout the country to determine possible transfer of assets, or other companies to be named in a suit.

* Obtain background information on an executive as a crucial part of performing due diligence.

* Explore possible conflicts of interest by looking for an executive's involvement with other companies.

* Check on the business affiliations of a prospective client.

BUSINESS FINDER
======== ======

SOURCE: American Business Information, Inc.

CONTENTS: Over 14 million U.S. and 1.7 million Canadian business listings compiled from the yellow pages of nearly 5,000 telephone directories. Contains over 9.5 million separate companies and 2 million professionals.

UPDATES: ABI continuously revises the information in the file, and updates the data from available telephone directories within six months after publication of the directory. Information America receives quarterly updates from ABI.

BUSINESS NEWS
======== ====

SOURCE: Comtex Scientific Corporation

CONTENTS: News stories from major national and international newswires, such as UPI, Kyodo, and TASS, press releases, and other various sources.

Stories are available from November 1989.

UPDATES: Twice Daily

Business News allows you to gather articles from major national and international newswires either by name, ticker symbol, industry or topic. Business News industry categories include:

1. Advertising (AD)	19. Electronics (EL)	37. Photography (PO)
2. Aerospace (AE)	20. Entertainment (EN)	38. Plastics (PL)
3. Agriculture (AG)	21. Environmental Srv (ES)	39. Prec Metals (PM)
4. Autos (AU)	22. Financial Srv (FS)	40. Publishing (PB)
5. Aviation (AV)	23. Food (FD)	41. Railroads (RR)
6. Banking (BK)	24. Forestry Prod (FP)	42. Real Estate (RE)
7. Beverages (BV)	25. Freight (FR)	43. Restaurant (RT)
8. Biotechnology (BI)	26. Health Care (HC)	44. Retail (RL)
9. Broadcasting (BR)	27. Industrial Prod (IP)	45. Rubber (RB)
10. Bldg Materials (BM)	28. Insurance (IN)	46. Ship Building (SB)
11. Business Srv (BS)	29. Machinery (MA)	47. Telecommun (TL)
12. Chemicals (CH)	30. Metals (ME)	48. Textiles (TX)
13. Computers (CM)	31. Mining (MI)	49. Tobacco (TB)
14. Construction (CN)	32. Nuclear Energy (NE)	50. Toys (TY)
15. Consumer Prod (CP)	33. Office Equipment (OE)	51. Travel Srv (TR)
16. Defense Contrt (DC)	34. Personal Care (PC)	52. Trucks (TK)
17. Education Srv (ED)	35. Petroleum Prod (PT)	53. Utilities (UT)
18. Electronic Publ (EP)	36. Pharmaceuticals (PH)	

BANKRUPTCY RECORDS
========== =======

SOURCE: The Bankruptcy Records are compiled for Information America from the official records at the U.S. Bankruptcy Courts. These records contain all publicly available cases filed in the following states: California, Georgia - Northern District (Atlanta and Gainesville only), New Jersey, Pennsylvania - Eastern District, and Texas.

CONTENTS: Bankruptcy records for both individuals and businesses are available. The records include debtor names, case number, location and date of filing, chapter number and more.

UPDATED: Weekly (California, Georgia, Pennsylvania, and Texas)
Bi-weekly (New Jersey)

You may select bankruptcy records by debtor name, social security/FEIN number or by case number.

SEC FILINGS
=== =======

SOURCE: SEC Online, Inc.

CONTENTS: Full text documents filed with the Securities and Exchange Commission by public companies traded on the New York and American Stock Exchanges as well as selected National Market System companies from NASDAQ. The documents available online - 10-Ks, 10-Qs, Annual Reports, Proxy Statements, and foreign company 20-Fs - contain all footnotes and selected exhibits. A Company Profile is also included that summarizes basic corporate information.

EFFECTIVE DATE: Information current from 07-01-1987.

UPDATES: Information America receives updates weekly from SEC Online.

Searches may be performed by company name or ticker symbol.

Notes on Information America
~~~~~ ~~ ~~~~~~~~~~~ ~~~~~~~

We mentioned that usernames beginning with "BIDA" are recognizable to the IA system as IA accounts (as opposed to shell accounts). More than likely, other usernames are also valid as IA accounts.

As with most systems, IA passwords are often easy to guess. Initial passwords, which are assigned when an account is first created, are usually composed of the account holder's first name, or first name plus a middle or last initial. In some cases, the password is made up of the digits in the username plus the first name of the account holder. In other cases, the password is two random letters plus a two-digit number (ex: PG13). If users are ever encouraged to change their password from its initial value, they rarely seem to do so.

You've probably noticed that IA has specific operating times (Eastern Standard Time). Most of IA's functions are inoperable during weekends and holidays and outside those specific operating hours. Occasionally on weekends, IA itself is down. Or more interestingly -- particularly on weekends -- the IA interactive environment will malfunction, dropping you into the VAX shell.

IA's clients are mostly lawyers and paralegals working at legal firms, but the FBI is also a major IA client. Television programs in the 60s and 70s which depicted an FBI "Big Brother" computer system scared the public enough so that it and the Congress have continually resisted efforts by the FBI to
~~~~~

implement such a system. In the mid 80s, for example, Congress voted against the implementation of an FBI computer system which would allow them to monitor telephone calls. Information America is the perfect solution for the FBI's bureaucratic quandary.

IA has existed for at least two and a half years, but has remained relatively unknown to the Telecom community until last year when MoD began using IA's People Finder to locate and terrorize people. IA's low profile isn't surprising; public backlash against Lotus' "MarketPlace" CD ROM -- which contained marketing information on only a few million people at most -- forced Lotus to abandon its project altogether after having invested tens of thousands of dollars in advertising alone, just as it was about to release MarketPlace. What Lotus was doing wasn't unusual; large direct marketing firms, like National Demographics & Lifestyles (NDL) have been somewhat covertly marketing consumer names and information on CD ROM for years (with information such as how many telephones you have; the approximate ages of your household's members; the gender of the household head; the number and type of cars your household has; what the mortgage value on your house is; estimated incomes for the heads of the household, etc...). The difference was that Lotus was offering their CD ROM commercially so that anybody could, as the public claimed, have the power of "Big Brother" at their fingertips. If the public knew about Information America, knew that anyone could tap its eye-spy capabilities, the outrage would be tremendous.

To market its database services, IA seems to have adopted a grass-roots kind of approach. IA employs liaisons in major metropolitan cities whose job it is to research and contact prospective clients -- lawyers, for example. We are unaware of any advertising in specialized journals.

We take for granted the existence of government-run databases which contain even more detailed information on Americans than IA possesses. Even so, those databases are considerably smaller, and what's more, they're well-regulated: the agencies that run them accountable by Law. The potential for abuse by a system like Information America -- devoid of any checks and balances -- is spectacular. MoD has already demonstrated this to a small extent. The same technology advances which were supposed to make at-home shopping a convenience and tailor marketing to your needs have now made surveilling you cost-effective, accurate and as easy as touching a key.

One of the least reported items to come to light out of the Iran/Contra proceedings was that, as head of the Federal Emergency Management Administration (FEMA) -- the organization which coordinates relief efforts across the United States during natural disasters -- Oliver North had drawn up FEMA contingency plans of a different sort: in the event of war in Central America, the Constitution was to be suspended and FEMA was to round up aliens (particularly Hispanics) and US Citizens considered "subversive," and interrogate them in Manzanar-like camps. Databases like Information America would no doubt have been employed in locating the whereabouts of these people.

The importance of Information America isn't what it can do for you; rather, what can be done with it to you.

- -

White Knight and I can be reached at WKnight@ATDT.ORG and Omega@ATDT.ORG, respectively. Additionally, we may be reached on Demon Roach Underground or Pure Nihilism. We welcome any questions or comments you may have -- especially any new information you may be able to add. Please do not contact us asking for accounts or passwords.

```
 _____                                                    _____
/   / \                                                  /   / \
(  5/5  )          BEATING THE RADAR RAP                 (  5/5  )
 \_/___/                                                  \_/___/
```

Part 1 of 2 : "Your Day in Court"

by Dispater

Introduction

Welcome to the first of two parts in a series designed to inform you about some of the aspects (both legal and technical) concerning traffic radar. The second part will appear in Phrack 38. I recommend you read both parts before attempting to apply the information you learn from this file.

Any hacker will tell you to ALWAYS find out as much as you possibly can about any endeavor and weigh the risks before you act. For most of us driving is something that we must do in order to have a career, get to school, and enjoy ourselves. Therefore it is essential to know the rules of the road and to know what will happen to you when you make a mistake. For the majority of us, this mistake means being given a speeding ticket or some type of moving violation.

This file will explain how to handle the situation should you ever need to go to court over a speeding ticket. I intend to provide you with a basic background so that the odds are a little more even.

One of the nasty things about traffic court is that for some reason, the burden of proof has flip-flopped from the state having to prove you are guilty (the way it is supposed to be) to the defendant having to prove that he/she is innocent.

First of all you are not alone in your quest to seek justice. Most judges are not evil and hateful. If you come into court, neatly dressed (not fancy, just look like a "semi-normal" person.), well informed of the issue, courteous, and acting a little humbled by the experience, the judge may lean a little more to your side. If you go to court, you will see a number of idiots who will stand up in front of the judge and argue or say "I wasn't doin' nothin'. I was just bein' harassed. I'm right and this pig was wrong. Nyah!" Obviously, the judge will not take kindly to this type of behavior. Would you?

In order to be informed, I HIGHLY recommend that you get in touch with the:

National Motorists Association
6678 Pertzborn Rd.
Dane, WI 53529
Phone : 1-800-882-2785

Membership: $20 student
per year $35 everyone else

The NMA provides a great deal of resources to those of use who drive. They provide (with membership) a legal resource kit for a rental fee of around $20.00 a month. This kit consists of 2 video tapes, 2 books, and a HUGE stack of information. Much of the "HUGE stack of information" consists of precedent cases in which the defense won, ALL radar gun manuals, lots of related news articles, error analysis information on vascar and other useful tidbits of information. It is excellent and I urge anyone who drives to get involved. The NMA, among other things, is the nice name for the "anti-55 people." They claim that it is up to the local governments and states to come up with their own speed limits. It's not Washington's job to tell the rest of us how to live!

The last thing I want to mention is that this is NOT a comprehensive file. Reading this will NOT make you a lawyer. If you can afford a lawyer, hire one. It is intended for people like me who can't afford a lawyer but who have some intelligence and guile in their personal make up. There's more than one way to skin a cat (cop) and you should NOT take this as a word for word way to proceed if you get nabbed for speeding. I intend for this to be the basis for building a good foundation for a case and to give you some ideas on how you might want to proceed. Do not go into the court room half-cocked. A good lawyer always knows the outcome of a case before he steps into the court room.

| You Get Busted! |

So the red lights are blinking behind you and your radar detector is going wild because you weren't paying attention because you were too busy messing with the radio and jamming to MC 900' Jesus so loudly that it shakes the widows of the car next to you. The first thing you want to do is pull over immediately! Don't try to be an bad ass and out run them. In most cases the cop's car can go faster than yours and besides, he has a radio. After you pull over, just hand him what ever he asks for and play in his desire to be "in control". Always say, "Yes sir" and "No sir" They LOVE that. Be as NICE as you can. Act "humbled". I know this may sound difficult but just TRY. ALL and I mean ALL people that become law enforcement officials have taken that job because they have some personality disorder that they NEED to feel in control of others and a NEED for others to respect them. This is a weakness in their personality, in my opinion. Anyway, If he just had a good round of golf that day, he may only write you a warning. If he still insists on writing you a ticket, he will at least know that you will not be a threat to him. ALL police officers, especially in large urban areas, will always approach your car as though you are going to shoot them. Make the officer thinks you are nice person (for the moment) and that your just weren't paying attention and you made a mistake. Again, as soon as you prove to him you are not a threat, he will relax and things will go much easier for you. I ALWAYS do this and the officer is actually NICE back to me most of the time. Even though his first impression is "long haired kid in a hot rod car wearing a Metallica shirt," the encounter usually ends with a "Have a nice day." or a "Just make sure you be careful now. ok?"

NOTE: If you are pulled over by a bull-dyke female cop, you are totally fucked. Social engineering is totally useless. ALL and I mean ALL bitch cops are just looking to prove something. They have a bad attitude because the "old boy" network back at the station doesn't like them and they think that most males will look on them as less of an authority figure merely because they are female, if they do not compensate (overcompensate) for the fact that they are women. They think that they will be challenged more often than not by you. I have yet to ever meet a NICE female cop. Lets face it, if they were NICE they would probably be an attorney or something. If you are women police officer reading this and you are not like what I have just described in the above paragraph then just ignore it and tell your cohorts to adjust the attitude!

Continuing on...As you are sitting there with everyone slowing down to take a look at you, make note of EVERYTHING! Write down the following:

1) Location (intersections, curves, condition of the road)
2) Weather (rain, fog, snow : all hinder traffic radar)
3) Traffic and all types of vehicles present (large trucks?)
4) Time (rush hour?)
5) Buildings present (airport? radio station? bank? microwave towers? power lines? hospital? telephone office?)
6) Officer's attitude (if he's angry this will play in your favor later)
7) Etc (anything else I failed to list here)

| Your Ticket and Pre-Trial Experiences |

So. Now in your possession you have a little gift from whomever had a bad day at work. The first thing you will want to do is make sure that all the information on the ticket is correct. If it is not, make sure that you take note of this and be sure to mention it as soon as your trial begins! You might be able to get off on a technicality. Another thing to check for is to make sure that the officer didn't write any little messages to the judge on the back of the ticket. If he wrote "radar detector." or some other irrelevant evidence, make sure you point out to the judge that that the speeding ticket is inadmissible as evidence in court due to the fact that it contains information that does not pertain to the case. The idea behind this is that most people that are caught speeding have radar detectors. Therefore, the cop will try to play on this fact in an indirect way. Even though this evidence is irrelevant, he will attempt to submit it. If the judge is cool, you'll get off on a technicality. Other ways to get off on technicalities is to make sure that EVERY tidbit of information is CORRECT. Incorrect information is a great way to get off. This is a

"procedural error" and might get the case dismissed. Continuing on....

Ok, so the ticket says you have to appear in court December 21st at 4:00. All this means is that if you wish to pay the ticket you must do so by this time and date. This does not usually mean you will actually go to court on this date. What you do next is go to the clerk's office and hand the lady behind the counter the ticket and say that you wish to contest it. They will set up a date (usually much later in the year sometimes a YEAR LATER if things are really backed up) and give you a piece of paper that you must bring to court with you. I highly suggest to everyone to ALWAYS, ALWAYS, ALWAYS contest a ticket. Hell, you have to pay court fees whether you show up or not so you might as well go, right? The point is to make them work for your money!

One good plan of action is to go to court a few weeks ahead of time and observe how proceedings work in your local court room. Just tell the bailiff that you are a criminal justice major and want to see how traffic court works and observe what REALLY goes on instead of reading it in a text book. If you are really clever, you might just want to ask one of the cops if you can go out and watch how police officers bust people speeding. Use the oldest, most classic social engineering maneuver ever invented, "It's for a paper for class." Let them think you are interested in becoming a cop. I don't care what they do or who they are, if someone comes up to them and appears to take interest in their profession, they will always be flattered. Always flatter the hell out of anyone you want to engineer!

The first thing you want to do before actually going to court yourself, is to not go to court. About a week before the trial or less, call the clerk's office and ask for a "continuance." Tell them that your boss told you that you have to go out of town the day of the trial and they will schedule you a new trail date. This is important because most police officers are less willing to show up. Thus if he's not there to prosecute you, you get off!

| Here come de Judge! Here come de Judge! |

Ok, so you're now sitting there in the presence of the other poor idiots that are in a similar predicament as you are. As you are sitting there sweating your ass off (being this is your first time in court, hopefully) Make sure you make note of other people's cases. What do the officers say when someone mentions traffic radar? See above above paragraph about testing the water a little. I have obtained a ton of information on how departments REALLY operate when they know I'm not there to pressure them. Use the lame statements the officers make against other officers and the rest of the department, when it's your turn. One time, before it was my turn I watched this one cop say, "The radar units are calibrated by the manufacturer and sent to us." Needless to say, I won that case!

Now the bailiff calls out, STATE OF TEXAS v. MR. OFFENDER! By this time you should know the routine. As soon as the judge opens things up to you ask him/her if you can examine the witness. They will say, "yes." Here is where you begin to make your case.

- -

PRELIMINARY QUESTIONS : "What?!?!?!" This is what the cop has going on inside his head right now. You are no longer the innocent fool you appeared to be in your car? He immediately raises his guard and you must lower it my placing a few questions to him and wearing him down. This part of the questioning is done to see if he can remember the exact circumstances under which he pulled you over and to get him used to you taking control of the interrogation.

A. What type of radar were you using on the date the citation was issued?

- Make sure he gives you the model name and number. Answers like "traffic radar or Doppler radar" should not be permitted.

B. Please relate the facts concerning the citation as you remember them.

- Make note if anything differs from what you remember to be true.

C. Was your audio doppler engaged at the time the citation was issued?

- If he says he doesn't know what that is, he hasn't been trained! The hand held units. (Speedgun series don't have audio doppler!) This is a good question to trip him up on! If he says he had it engaged, merely whip out the manual and ask him if to point out where the heck it is. OR you can ask to subpoena the unit to court and ask him to find it!

D. What speed was your audio alarm set for?

- If he says he doesn't know what that is, he hasn't been trained!

E. Was your automatic speed lock engaged?

- If yes, you have already started to build your case that they made an error. If not then keep going.

F. Were you stationary or moving at the time your radar unit's alarm went off?

- Who cares unless you want to go off and provide some kind of "cosine-error" evidence later.

G. Was I coming toward you or away from you?

- Again, this doesn't matter

H. Did you see me prior to the time your radar's audio alarm went off?

- This is important, you are in effect asking him if he took a traffic history before he set up camp behind the bushes waiting to pop people.

I. Could you estimate my speed?

Irrelevant

J. What was the apparent speed?

Irrelevant

K. How many seconds did it take you to react between the time you first saw my vehicle and the time your audio alarm sounded?

- This doesn't matter, unless it was a case of you coming around a curve or over a hill and old Smokey is there waiting to bust the first thing that makes his little machine go beep. He must have tracked you long enough to get a good reading. This should be about 5-8 seconds to take into account spurious readings. If he didn't wait that long he is ignoring his training.

L. Using this paper could you make a map of the area?

- Most of the time to police officer will be unable to remember details of the surroundings since he hands out many tickets a day. This is a good place to establish doubt.

- -

ESTABLISH THE OFFICER'S LEVEL OF QUALIFICATIONS: This is done in an attempt to make the police officer appear as unqualified as possible. Make the officer appear to have as little training as possible and be as unfamiliar with the radar unit as possible. The bigger a fool you can make the cop out to be the more points you'll score with the judge.

A. How long have you been a police officer?

Irrelevant unless he's just come straight from the academy

B. How long have you been operating radar?

Irrelevant unless it's a year or less.

C. Have you received formal training on the operation of radar?

- If NO then you've hit pay-dirt.

D. Under what circumstances did you receive this training?

Irrelevant unless he says, "in the locker room." In this case he may be on your side.

E. How many hours of classroom training did you receive?

- This is an important answer. If he says four or less, he's probably not qualified. Make note.

F. How long ago did you receive this training?

Irrelevant unless the answer is five or six years ago. He may be out of practice and probably wasn't trained on the model he used to bust you.

G. Who taught the class?

- If it was his sergeant, you have a case of the blind leading the blind. If it was the radar manufacturer you have a potentially biased source since the manufacturer will do anything to sell it's merchandise! If he was SENT to the manufacturer's school he's better than most.

H. Since initial training, have you had any brush-up courses?

- If he says yes, he's full of more shit than you are. Ask who taught them and when they were.

I. Do you believe yourself to be a competent radar operator?

- Sure he does

J. Do you hold a certification?

- In some states he MUST be trained at the manufacturer's school. If he says his sergeant certified him. You may be able to walk out of court right there. It's a case of the blind leading the blind.

K. Did you receive your initial training with the model (the one he popped you with)?

- If his formal training was with another unit, you've hit pay-dirt again!

L. How many one-on-one sessions of field training did he receive?

- Answers like, "I rode with another officer while he wrote tickets." are not good. Keep pressing him on this issue. Most likely he did not have this type of training unless it was done by a factory representative and then there were three other officers in the car at the time.

- -

ESTABLISH THE LEVEL OF TRUST THE OFFICER PLACES IN HIS RADAR: These questions are used in an attempt to make it appear as though the police officer himself questions the reliability of traffic radar. This is where things get fun and he could even purger himself if he's not careful. In which case you win again!

A. Do you believe the (radar unit he popped you with) to be a good unit?

- Of course he does. If he doesn't he may be on your side.

B. Have you ever encountered problems with the (model) radar?

- If he says yes, make sure he tells you details, and not simply, "It quit working one day."

C. Are you permanently assigned to one specific radar unit?

- They will always switch around. He will most likely say that he uses the same brand name but different models.

D. Do you believe there to be differences between brands of radar units or models? Will one have idiosyncrasies that others may not have?

- He will most likely say that they all work alike. If he says he has differences make sure he tells you exactly what they are and how he noticed them.

E. Do you believe that the (model radar) ever gives spurious or false readings?

- If he says "no." Make sure you have documented evidence of this. (see above information on the NSA) This is a real good way to make him look like an idiot. Make sure that you repeat the question and emphasis the word "NEVER." After he says no again, hand the document to the judge and say something to the effect that, "I have written evidence right here that was written by an independent engineering firm that proves that (model radar) does have the capability to give false readings. Now, in a court of law you are not permitted to defend yourself while examining the witness, however, since you are not an attorney. The judge may permit you do submit your testimony.

  If the officer says "yes" he has seen false readings, ask him what percentage of the time it does give spurious readings. In the case STATE OF WISCONSIN vs HANSEN, in which HANSEN prevailed. It was proven that radar can give false readings up to 20% of the time.

F. Do you believe you can always tell the radar unit is giving a spurious reading?

- He will always say he can. If he says, "no" then you've already established reasonable doubt. When he says "yes," then proceed with the next two questions and then come back to this one again.

G. Is there is a special number that appears on the screen that indicates a false reading.

- Not!

H. Does the unit give some visual indication that the reading is suspected to be false?

- Not! (Believe it or not! The very first case I went to defend myself, the idiot cop said that there was an "indicator light that noted when there is radar disturbance in the area." HAHAHAHA!!! What a joke. I asked him to point it out to me and of course he couldn't. Therefore he just lied under oath. He fucked himself hard! Needless to say the judge wasn't too pleased, to see a police officer lying either! ;-)

I. How then can you tell that the reading you are getting is spurious?

- He will answer that there is no target or that the car is obviously not speeding.

J. You said that there isn't some special speed or number that appears on the screen. All 86 mph speed readings are not spurious for example?

- Of course not.

K. So the spurious reading could be either 20mph or 70mph?

- Of course. If he says not, he is out of his league and attempting to evade answers.

L. The radar could give a speed of 20mph or 70mph, but you could see clearly, for example, that the car was going only 30mph?

- He should agree with that.

M. What if a car was going 55mph and you got a reading of 70mph? Is this possible?

- He should agree with that.

N. Assuming a car was approaching you at 55mph. You could recognize that?

- He'll probably say he could. If he does, keep going. If he says he could not then you've already established doubt.

O. If a car was approaching at 55mph and you get a reading of 56mph. Could you tell that it was a spurious reading?

- Of course not. At this point keep the pressure on by rapidly asking the question over and over again and increasing the false reading by one mph until he gives. If you've led the cop into this trap you are doing great! He is totally fucked if he answers either "yes" or "no." This is because you are establishing more doubt each time he says "no" and if he does say "yes" too soon he will appear to have some super-human quality!

- -

USE OF AUDIO DOPPLER, AUDIO ALARM, AND AUTOMATIC SPEED LOCK: All radar units include features designed to make the officer's job easier. The AUDIO DOPPLER can be turned down or off, as is usually done, therefore it contributes nothing to reliability. The AUDIO ALARM is a warning tone that tells the officer the radar unit has "got one", and it is built into all radar units. The officer must dial in a speed above which he wants the alarm to sound. The only way to disengage the alarm is to dial the speed to 99 mph or 199 mph on some models. The AUTOMATIC SPEED LOCK is the worst thing ever put in a radar unit. It automatically locks up a speed reading when one comes above the preset level. If the reading is spurious, the officer never knows it. Your goal here is to establish his normal operating habits. Later, you'll find out how he was using radar on the day he busted you.

A. Does your radar unit have an audio Doppler? That is a continuous audio single tone which converts the radar unit's Doppler shift into an audible signal?

- He will say his unit does, unless it's a Speedgun, in which case it does not. If it was a Speedgun jump to question "M".

B. Does the audio doppler have a volume control?

- Yes it does.

C. Do you ever use your audio doppler?

- If he says "yes" continue. If he says no skip to question `M`.

D. About what percent of the time will you listen to the audio doppler?

- note percent

E. When you operate your radar unit with audio doppler on do you operate it at full volume?

Heh, yea right!

F. At what volume do you operate it?

- The question can only be helpful if he says he operates it at a low volume. Try to ask him a few similar questions that will make him answer "low volume." IE: "I know that that tone get's awfully annoying doesn't it?"

G. Do you ever turn it off?

- Sure he does.

H. Why do you turn it off?

- Because it is irritating as hell!

I. Does the use of audio doppler ever interfere with your use of the police radio or your conversations with other officers?

- He should say it does.

J. So you operate with the audio doppler off about ___ percent of the time?

- Fill in the number that he gave you earlier.

K. Of the rest of the time, how often do you operate it with the volume on soft.

- (Note the percentage)

L. Do you consider the audio doppler an important tool to prevent operator error?

- Only important if he says "no".

M. Is your radar unit equipped with a dial that lets you select a speed above which an audio tone will sound if a violation speed is picked up?

- Yes, all radar units have this feature.

N. We'll call that feature the AUDIO ALARM. Do you commonly use that feature?

- He has to.

O. What percentage of the time do you use this?

- If he answers anything less than 100%, ask him how he disengages it. He would have to disassemble the whole radar unit.

P. If the speed limit on a highway is 55, what speed do you normally dial in as your pre-set violator speed?

- Note speed. The answer isn't critical.

Q. Do you find that feature to be a useful one for you?

- He'll probably say it's sometimes useful.

R. If a violation speed causes the alarm to sound, you need only reach over to lock in that speed, is that correct?

- That's how it works.

S. Does your radar unit also have a button or switch which permits the radar unit to automatically lock up the violation speed?

- Yes, it does.

T. Do you ever use that automatic speed lock function?

- If he says "no", repeat the question with an emphasis on the "ever" and look skeptical. If he still says no, skip to the next question section.

U. About what percent of the time do you use the automatic speed lock?

- Note percent.

V. Do you find that automatic speed lock convenient?

- Sure he does. That way he can read a magazine or take a nap while the radar unit does the for him!

W. Do you use the automatic speed lock for any other reason?

- Note reasons, if any.

X. Was the use of the automatic speed lock included in your training?

- Answer isn't important.

- -

ESTABLISHING WHETHER THE OFFICER USES A VISUAL BACK UP: When cops go to court, they have a "model testimony" used to establish their reasoning for giving out a ticket. One part of this testimony usually centers on the radar unit used only as a backup to their visual perception that you, the defendant, were traveling at a "high rate of speed" or at "X mph." Put in it simplest form, this is total hogwash. A trained officer can make a visual identification of speed at a distance of perhaps 500 feet. The radar can theoretically make that same speed determination at 5000 feet. The radar's alarm will sound many seconds before the policeman can make a visual speed determination. As it is, the cop will observation of a car will verify what the radar has already told him. THIS IS WRONG! The law states that "radar readings can ONLY be used as corroborative evidence." If the cop sees that the car is traveling slower than what the radar says, he will merely assume that the driver saw him and slowed down. The following questions are used to establish whether or not the cop did use visual back up, and trap him onto making a statement which can later be used against him!

A. I'm going to start this question by defining a term I call a "traffic history". A traffic history is the continuous observation of traffic by a police officer. If an officer takes a traffic history, it means he is CONTINUALLY WATCHING TRAFFIC; looking for speeders, drunken drivers, or any other offenders. Do you understand what I mean by a traffic history?

- If the officer doesn't understand, keep explaining until he does.

B. With regard to speeding tickets, an officer who says he normally takes a traffic history can say that he observes traffic patterns for a period of several seconds -- usually three to five seconds -- before he sees what he believes to be a speeding incident. That is, three to five seconds before his radar unit sounds its alarm. He then continues to observe traffic fora period of several seconds while he determines that a citation should be issued. Do you understand that definition of a traffic history as it applies to speeding tickets?

- The officer should understand.

C. Using that definition, have you EVER taken a traffic history prior to issuing a speeding citation?

- He will probably answer that he has. If he says no, see answer E.

D. About what percent of the time can you say you have taken a traffic history when you issue a speeding ticket?

- Note percent. It will probably be very high.

E. Do you believe it is important to take a traffic history in speeding cases?

- He'll probably say "yes." If he says no, you have a strong argument in court, namely that he had no visual backup; that he was relying solely on his radar unit. His "yes" answer, in conjunction with the fact that he didn't take one in your case, can be used against him in court.

F. At about what distance can you make a determination that a car is doing a certain number of miles per hour?

- Most policemen answer about 500. If he hedges or says it depends, set up a specific situation, for example, he is in the median strip of a level, straight, uncrowded highway. At what distance can he make a visual determination of the speed of an approaching car? If he says he still can't say, throw the 500 feet figure at him and see if he agrees. Shorten and lengthen the figure to get an estimate he can live with.

G. When you take this traffic history and make a visual assumption about speed, you do so BEFORE your radar unit has sounded its audio alarm?

- THIS IS A TRICK QUESTION. If he says "yes", he's in trouble because his radar unit's range is doubtlessly longer than his visual acuity.
  If he says "no", then he hasn't really taken a traffic history.
  If he says "yes", ask questions H and I.
  If he says "no", ask questions J, K, L, M, N, and O, P, Q, R.

H. Approximately what is the range of your radar unit?

- He'll probably say he doesn't know. Throw figures between 3,000 and 5,000 feet at him and see if he agrees with any of them. If he still doesn't know, ask if he'd be surprised to find out that his radar unit had a range of at least 3,000 feet. If he says yes to that question, you have just nailed him on a vital technical question.

I. But you still stick to your statement that the radar unit does not sound an alarm prior to your being able to recognize the true velocity of a car?

- Regardless of his answer, you've made your point.

J. Then you don't really take a traffic history.

- The neatest answer is "no", which he probably won't say. Instead, he'll say that sometimes it does and sometimes it doesn't. For the "sometimes it doesn't" answers, go back to questions H and I. For the "sometimes it does" answer, continue.

K. If the radar unit sounds an alarm before you've had a chance to ascertain that a car is speeding, how can you say you've taken a traffic history?

- He'll probably say it alerts him to look for a speeder.

L. Do you look down to see how fast the radar unit says a car is going?

- He'll probably he looks. If he says he doesn't look, tell him, "but you know a car is definitely going at least X mph over the speed limit?" To that, he has to answer yes.

M. Does the knowledge that the radar unit has already "got one" influence your judgement in making a visual determination of a car's speed? That is, will you be more likely to agree that a car is going a certain number of miles per hour after the radar has already said that it was going that speed?

- He should agree. If he doesn't, ask him why he doesn't just run his alarm setting up to 99 mph to make certain it never influences his judgement? His answer won't matter.

N. Would you be more inclined to believe that a car in the left lane of a four-lane highway was a speeder if you heard your audio alarm go off?

- If he's honest, he'll say yes. If he isn't, he'll say, "if it was passing another vehicle". Counter with "what if there wasn't a reference vehicle present, but the car was still in the left lane? If he still says "no", ask him again why he doesn't just run his alarm counter up to 99 mph.

O. If there was a car going slower than the speed limit in the right lane, and a car driving at the speed limit in the left lane apparently passing it, and your radar unit either malfunctioned or misread the target, might you mistakenly conclude that the car in the left lane was speeding and issue the driver a citation?

- If he's honest, he'll answer "yes", building your case for operator error. If he says "no", he could tell the car in the left lane wasn't speeding, you're back to question F.

P. If your radar unit said it had picked up a car going, say, 70 mph, and when you were able to make out its speed, it was clearly going the speed limit, would you be inclined to believe the motorist had seen you and quickly slowed down?

- The honest officer will say yes.

Q. Would you still issue the citation based on the radar reading?

- Again, he should say "yes".

R. Why do you set your alarm counter for a certain number of miles per hour over the speed limit?

- His answer may be that he was trained to do so (unusable), or that he needs it for special circumstances (worth following up). Any excuse will be lame.

- -

ESTABLISHING THE LEVEL OF KNOWLEDGE ABOUT BEAM WIDTH AND RANGE: Under HONEYCUTT, a police officer does not need to know the inner workings of his radar unit in order to have his testimony accepted by the court. The mistake is made by many persons challenging radar-backed speeding citations is to try and demonstrate to the court that they know more about radar than the cop that issued them a ticket.

It really doesn't matter how much you know about radar. All the court wants to know is how much the officer knows. Few judges have ever questioned the qualifications of the citing officer. Your job as a defendant is to make the judge do just exactly that! You will have to plant a seed of doubt in his/her mind by showing that in several key areas, the officer doesn't know fundamental aspects of radar.

A. With respect to everyday operation of your radar unit, do you know what its approximate range is?

- Depending on the model, the answer can range from 3,000 to 7,000 feet. Refer to second article in this series that will appear in the next exciting issue of Phrack!

B. At a distance of 1000 feet how wide is the radar beam?

C. About how far from the radar antenna will the beam be when it is width of one lane of traffic, or about 11 feet?

D. With what degree of certainty can you point your radar's antenna at, say, the left lane of oncoming traffic and at a distance of, say, 500 feet be focusing on just that lane of traffic?

- The answer is zero. Anything else and he is wrong.

E. In the stationary mode, you can lock the speed of traffic in either

direction, that is, you can flip the antenna to record traffic going away from you or traffic coming toward you. Is that correct?

- Yes it is.

F. Can your radar differentiate between traffic direction? For example, if you're setting along a expressway, and you have your radar unit pointed toward you oncoming traffic, will your radar unit pick up only oncoming traffic, or might it also pick up traffic on the other side of the median strip moving away from you?

- It will pick up traffic in either direction. Any other statement (e.g. "sometimes it does and sometimes it doesn't" is ignorance.)

G. In moving mode, can your radar pick up traffic both coming toward you and traffic moving away from you?

- The Speedgun 8 is the ONLY radar that can do this. It can only clock cars coming toward it. No other radar unit can do this!

H. [In the next two questions you will have to draw a picture. Draw a vertical roadway with a car (#) going up toward the top and the cops car oriented perpendicular to the road (<:=). Next draw a line that is perpendicular to the roadway (<---). This is the radar beam. You should have a slightly larger drawing :) that looks similar to the one to the left. Hold this up so that the judge and the cop can see it and ask the following question.]

```
   | . |
   | . |
   | . |
 <-------<:=
   | . |
   | .^|
   | .#|
```

In this diagram, the radar is held at right angles to the roadway. A north bound car driving at 55mph enters into the radar beam. Will the radar unit pick up the car?

- It cannot. There is NO doppler shift because there is no closing speed between the vehicle and the radar unit. If he answers correctly, skip to question "J".

I. [Again you need to draw a picture similar to the one above, but this time add a car going in the opposite direction, in the other lane of course! It should look something like the picture below. Now present this to the cop and the judges and ask the following: (Refer to this as fig. '2')]

```
   |#. |
   |~  |
   | . |
 <-------<:=
   | . |
   | .^|
   | .#|
```

In this diagram, two cars are approaching from opposite directions, with the radar unit sill pointed at right angles on the highway. The north bound car (right) is going 55mph. The southbound car (left) is going 65mph. Which car will the radar unit pick up and how will you be able to distinguish between the two?

- If he even thinks about answering this question he is an idiot. Neither car will register. (see question 'H')

J. What kind of things will stop the beam? Will underbrush stop the beam or can you get a reading through tall grass, weeds, and bushes?

- Radar will go through these things.

K. Are there circumstances under which you can obtain the speed of a vehicle you cannot see? For example, can you obtain the speed of a vehicle around a corner or over a hill?

- Not in this world.

L. Will your radar beam bounce off a metal surface such as a sign, a car, a ,metal building, or a steal or concrete overpass?

- Sure will.

M. What happens to the beam when it bounces off a metal object? Could it pick up the speed of a car at an angle to the direction you have the radar pointed?

- Yes it will.

N. Could a high power utility transmission line interfere with the radar unit?

- Yup.

O. Could airport radar or military radar interfere with the radar?

- Sure can.

P. Have you ever noticed interference from things like neon signs or street lights?

- Such things do produce interference

- -

FINAL QUESTIONS: By now you have either made a enemy of the officer (most likely outcome) or started him thinking about the incident (if he is a good police officer). The officer, of course, doesn't know what answers he got right and what ones he got wrong. Watch for variations between answers, or especially, any weakening in his determination that yours was the car which registered on the radar unit.

Questions 'N'-'Q' taken together represent critical procedural questions. It is important to differentiate between an internal calibration check (pushing a button) and an external check (holding a tuning fork to the antenna).

A. Officer (such and such), let's go back over your recollection of the incident one last time. Can you relate the facts concerning the citation as you remember them?

B. Was your audio Doppler engaged at the time of the incident? How loud or soft was it?

C. What speed was your audio alarm set for? Had you moved it up or down during your shift?

D. Was your automatic speed lock engaged?

E. Were you using a manual on-off switch?

F. Were you in a stationary or moving mode at the time?

G. Was the defendant coming or going away from you?

H. Did you see other vehicles either in front of or behind the defendant? Were they varied in size? Were they varied in direction of travel?

I. Was there traffic moving in the same direction as you? (if moving)

J. Did you see the defendant prior to the time your audio alarm sounded?

K. Were you able to obtain an approximate speed reading based on your visual identification? What was your point of reference?

L. How many seconds elapsed between the time you first observed the defendant and the time your audio alarm sounded?

M. Were there any power lines in the area? Cars or homes with CB antennas? Buildings with two-way radio antennas? Had you been talking on your radio?

N. Regarding calibration of the radar unit, using the INTERNAL calibration function, at what times before and after the citation did you check the radar?

O. Using an "external tuning fork", at what times before and after the citation did you check your radar?

P. In your estimation, what is the difference between the internal and external calibration function?

Q. Do you consider one of the calibration checks to be a more accurate indicator of accuracy? Which one?

| Closing Arguments | If you have done well you will have established a great deal of doubt in the judges mind as to the capability of the officer in question to operate a radar unit. You have have set him/her thinking about the "big picture." That is, "Just how accurate is traffic radars?" This is what you want to achieve but it must be done in subtle way.

You aren't out of the hole yet! Now that you have established doubt in the judge's mind you MUST provide testimony that will TIE all the testimony the officer gave in with YOURS. This is where you have to do the thinking on your own. It should be very obvious how to do this. Your job is to break down the testimony. You are looking for 1) Procedural errors, 2) Lack of knowledge on the part of the officer, 3) Possible radars errors. If you can get him on two of the three, you are set!

Procedural errors include things like the previously mentioned incorrect citation. Other procedural errors that are easy to play on is this. The officer must use an external tuning that is certified as to it's accuracy in testing the radar unit immediately before he gives a citation. Two court cases that are examples of this are WISCONSIN v. HANSEN and MINNESOTA v. GERDES. Simply put, if you are in need of throwing around some weight in court, just cite these two cases. They are great!

Ignorance on the part of the officer is pretty obvious. If he messes up the questions, he is ignorant. They are all pretty simple, I think. If a cop does things like, uses his automatic speed lock or doesn't use his audio doppler, he is blatantly ignoring his training. Most of the time they will bring a copy of their training manual to court. Just point it out to them!

There are too many potential radar errors to mention here. You must try to locate them in the vicinity of where you encounter your ticket. Anything that transmits on uncommon frequencies is great to note. (e.g. burglar alarms, garage doors, CB's, Ham Radio, rain, fog, police radio, hospitals, etc, etc.)

In closing, I hope you found this information useful and look forward to the second part in my series, "Beating the Radar Rap: The Technical Side." This will be a file where I go into picking apart the actual flaws that specific radar guns have.

Card-O-Rama: Magnetic Stripe Technology and Beyond
or
"A Day in the Life of a Flux Reversal"

Written by

oooOO Count Zero OOooo
Restricted Data Transmissions

November 22, 1992

Look in your wallet. Chances are you own at least 3 cards that have magnetic stripes on the back. ATM cards, credit cards, calling cards, frequent flyer cards, ID cards, passcards,...cards, cards, cards! And chances are you have NO idea what information is on those stripes or how they are encoded. This detailed document will enlighten you and hopefully spark your interest in this fascinating field. None of this info is "illegal"...but MANY organizations (the government, credit card companies, security firms, etc.) would rather keep you in the dark. Also, many people will IMMEDIATELY assume that you are a CRIMINAL if you merely "mention" that you are "interested in how magnetic stripe cards work." Watch yourself, ok? Just remember that there is nothing wrong with wanting to know how things work, although in our present society, you may be labelled a "deviant" (or worse, <gasp> a "hacker")!

Anyway, I will explain in detail how magstripes are encoded and give several examples of the data found on some common cards. I will also cover the technical theory behind magnetic encoding, and discuss magnetic encoding alternatives to magstripes (Wiegand, barium ferrite). Non-magnetic card technology (bar code, infrared, etc.) will be described. Finally, there will be an end discussion on security systems and the ramifications of emergent "smartcard" and biometric technologies.

DISCLAIMER

Use this info to EXPLORE, not to EXPLOIT. This text is presented for informational purposes only, and I cannot be held responsible for anything you do or any consequences thereof. I do not condone fraud, larceny, or any other criminal activities.

A WARNING

Lately, I've noticed a few "books" and "magazines" for sale that were FILLED with FILES on a variety of computer topics. These file were originally released into the Net with the intention of distributing them for FREE. HOWEVER, these files are now being PACKAGED and sold FOR PROFIT. This really pisses me off. I am writing this to be SHARED for FREE, and I ask no payment. Feel free to reprint this in hardcopy format and sell it if you must, but NO PROFITS must be made. Not a fucking DIME! If ANYONE reprints this file and tries to sell it FOR A PROFIT, I will hunt you down and make your life miserable. How? Use your imagination. The reality will be worse.

** MAGSTRIPE FIELDS, HEADS, ENCODING/READING **

Now, I'll get down to business!

First, I am going to explain the basics behind fields, heads, encoding and reading. Try and absorb the THEORY behind encoding/reading. This will help you greatly if you ever decide to build your own encoder/reader from scratch (more on that later). FERROMAGNETIC materials are substances that retain magnetism after an external magnetizing field is removed. This principle is the basis of ALL magnetic recording and playback. Magnetic POLES always occur in pairs within magnetized material, and MAGNETIC FLUX lines emerge from the NORTH pole and terminate at the SOUTH. The elemental parts of MAGSTRIPES are ferromagnetic particles about 20 millionths of an inch long, each of which acts like a tiny bar magnet. These particles are rigidly held together by a resin binder. The magnetic particles are made by companies which make coloring

pigments for the paint industry, and are usually called pigments. When making the magstripe media, the elemental magnetic particles are aligned with their North-South axes parallel to the magnetic stripe by means of an external magnetic fields while the binder hardens.

These particles are actually permanent bar magnets with TWO STABLE POLARITIES. If a magnetic particle is placed in a strong external magnetic field of the opposite polarity, it will FLIP its own polarity (North becomes South, South becomes North). The external magnetic field strength required to produce this flip is called the COERCIVE FORCE, or COERCIVITY of the particle. Magnetic pigments are available in a variety of coercivities (more on that later on).

An unencoded magstripe is actually a series of North-South magnetic domains (see Figure 1). The adjacent N-S fluxes merge, and the entire stripe acts as a single bar magnet with North and South poles at its ends.

```
Figure 1:              N-S.N-S.N-S.N-S.N-S.N-S.N-S.N-S.N-S <-particles in stripe
---------
       represented as-> N-----------------------------S
```

However, if a S-S interface is created somewhere on the stripe, the fluxes will REPEL, and we get a concentration of flux lines around the S-S interface (same with N-N interface). ENCODING consists of creating S-S and N-N interfaces, and READING consists of (you guessed it) detecting 'em. The S-S and N-N interfaces are called FLUX REVERSALS.

```
                             ||| ||| <-flux lines
Figure 2:      N------------N-N-S-S-----------------S
---------     flux lines -> ||| |||
```

The external magnetic field used to flip the polarities is produced by a SOLENOID, which can REVERSE its polarity by reversing the direction of CURRENT. An ENCODING head solenoid looks like a bar magnet bent into the shape of a ring so that the North/South poles are very close and face each other across a tiny gap. The field of the solenoid is concentrated across this gap, and when elemental magnetic particles of the magstripe are exposed to this field, they polarize to the OPPOSITE (unlike poles attract). Movement of the stripe past the solenoid gap during which the polarity of the solenoid is REVERSED will produce a SINGLE flux reversal (see Figure 3). To erase a magstripe, the encoding head is held at a CONSTANT polarity and the ENTIRE stripe is moved past it. No flux reversals, no data.

```
                               | |  <----wires leading to solenoid
                               | |       (wrapped around ring)
                              /-|-|-\
                             /       \
Figure 3:                    |       | <----solenoid (has JUST changed polarity)

---------                    \       /
                              \ N S / <---gap in ring.. NS polarity across gap
      N----------------------SS-N-------------------------S
                              ^^
                  <<<<<-direction of stripe movement

          S-S flux reversal created at trailing edge of solenoid!
```

So, we now know that flux reversals are only created the INSTANT the solenoid CHANGES its POLARITY. If the solenoid in Figure 3 were to remain at its current polarity, no further flux reversals would be created as the magstripe moves from right to left. But, if we were to change the solenoid gap polarity >from NS to *SN*, then (you guessed it) a *N-N* flux reversal would instantly be created. Just remember, for each and every reversal in solenoid polarity, a single flux reversal is created (commit it to memory). An encoded magstripe is therefore just a series of flux reversals (NN followed by SS followed by NN).

DATA! DATA! DATA! That's what you want! How the hell are flux reversals read and interpreted as data? Another solenoid called a READ HEAD is used to detect these flux reversals. The read head operates on the principle of ELECTROMAGNETIC RECIPROCITY: current passing thru a solenoid produces a magnetic field at the gap, therefore, the presence of a magnetic field at the gap of a solenoid coil will *produce a current in the coil*! The strongest magnetic fields on a magstripe are at the points of flux reversals. These are detected as voltage peaks by the reader, with +/- voltages corresponding to NN/SS flux reversals (remember, flux reversals come in 2 flavors).

See Figure 4.

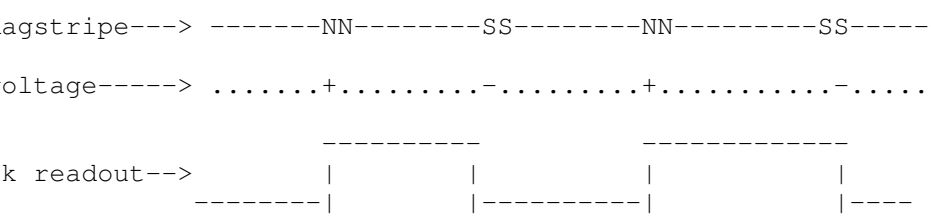
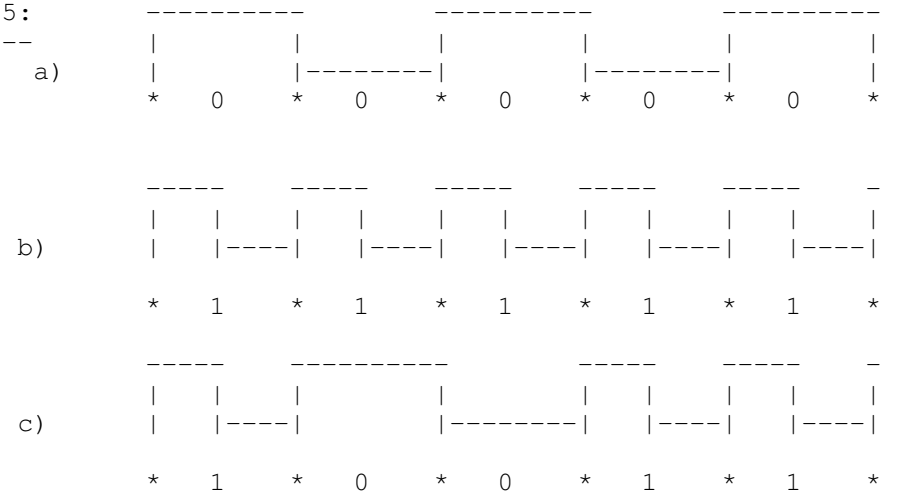


Figure 4:

The "peak readout" square waveform is critical. Notice that the voltage peak remains the same until a new flux reversal is encountered.

Now, how can we encode DATA? The most common technique used is known as Aiken Biphase, or "two-frequency coherent-phase encoding" (sounds impressive, eh?). First, digest the diagrams in Figure 5.

Figure 5:



There you have it. Data is encoded in "bit cells," the frequency of which is the frequency of '0' signals. '1' signals are exactly TWICE the frequency of '0' signals. Therefore, while the actual frequency of the data passing the read head will vary due to swipe speed, data density, etc, the '1' frequency will ALWAYS be TWICE the '0' frequency. Figure 5C shows exactly how '1' and '0' data exists side by side.

We're getting closer to read DATA! Now, we're all familiar with binary and how numbers and letters can be represented in binary fashion very easily. There are obviously an *infinite* number of possible standards, but thankfully the American National Standards Institute (ANSI) and the International Standards Organization (ISO) have chosen 2 standards. The first is

** ANSI/ISO BCD Data format **

This is a 5-bit Binary Coded Decimal format. It uses a 16-character set, which uses 4 of the 5 available bits. The 5th bit is an ODD parity bit, which means there must be an odd number of 1's in the 5-bit character..the parity bit will "force" the total to be odd. Also, the Least Significant Bits are read FIRST on the strip. See Figure 6.

The sum of the 1's in each case is odd, thanks to the parity bit. If the read system adds up the 5 bits and gets an EVEN number, it flags the read as ERROR, and you got to scan the card again (I *know* a lot of you out there *already* understand parity, but I got to cover all the bases...not everyone sleeps with their modem and can recite the entire AT command set at will, you know). See Figure 6 for details of ANSI/ISO BCD.

Figure 6: ANSI/ISO BCD Data Format
---

* Remember that b1 (bit #1) is the LSB (least significant bit)!
* The LSB is read FIRST!
* Hexadecimal conversions of the Data Bits are given in parenthesis (xH).

--Data Bits--				Parity		
b1	b2	b3	b4	b5	Character	Function
0	0	0	0	1	0 (0H)	Data
1	0	0	0	0	1 (1H)	"
0	1	0	0	0	2 (2H)	"
1	1	0	0	1	3 (3H)	"
0	0	1	0	0	4 (4H)	"
1	0	1	0	1	5 (5H)	"
0	1	1	0	1	6 (6H)	"
1	1	1	0	0	7 (7H)	"
0	0	0	1	0	8 (8H)	"
1	0	0	1	1	9 (9H)	"
0	1	0	1	1	: (AH)	Control
1	1	0	1	0	; (BH)	Start Sentinel
0	0	1	1	1	< (CH)	Control
1	0	1	1	0	= (DH)	Field Separator
0	1	1	1	0	> (EH)	Control
1	1	1	1	1	? (FH)	End Sentinel

***** 16 Character 5-bit Set *****
10 Numeric Data Characters
3 Framing/Field Characters
3 Control Characters

The magstripe begins with a string of Zero bit-cells to permit the self-clocking feature of biphase to "sync" and begin decoding. A "Start Sentinel" character then tells the reformatting process where to start grouping the decoded bitstream into groups of 5 bits each. At the end of the data, an "End Sentinel" is encountered, which is followed by an "Longitudinal Redundancy Check (LRC) character. The LRC is a parity check for the sums of all b1, b2, b3, and b4 data bits of all preceding characters. The LRC character will catch the remote error that could occur if an individual character had two compensating errors in its bit pattern (which would fool the 5th-bit parity check).

The START SENTINEL, END SENTINEL, and LRC are collectively called "Framing Characters", and are discarded at the end of the reformatting process.

** ANSI/ISO ALPHA Data Format **

Alphanumeric data can also be encoded on magstripes. The second ANSI/ISO data format is ALPHA (alphanumeric) and involves a 7-bit character set with 64 characters. As before, an odd parity bit is added to the required 6 data bits for each of the 64 characters. See Figure 7.

Figure 7:

ANSI/ISO ALPHA Data Format

* Remember that b1 (bit #1) is the LSB (least significant bit)!

* The LSB is read FIRST!
* Hexadecimal conversions of the Data Bits are given in parenthesis (xH).

------Data Bits-------						Parity		
b1	b2	b3	b4	b5	b6	b7	Character	Function
0	0	0	0	0	0	1	space (0H)	Special
1	0	0	0	0	0	0	! (1H)	"
0	1	0	0	0	0	0	" (2H)	"
1	1	0	0	0	0	1	# (3H)	"
0	0	1	0	0	0	0	$ (4H)	"
1	0	1	0	0	0	1	% (5H)	Start Sentinel
0	1	1	0	0	0	1	& (6H)	Special
1	1	1	0	0	0	0	’ (7H)	"
0	0	0	1	0	0	0	((8H)	"
1	0	0	1	0	0	1	) (9H)	"
0	1	0	1	0	0	1	* (AH)	"
1	1	0	1	0	0	0	+ (BH)	"
0	0	1	1	0	0	1	, (CH)	"
1	0	1	1	0	0	0	- (DH)	"
0	1	1	1	0	0	0	. (EH)	"
1	1	1	1	0	0	1	/ (FH)	"
0	0	0	0	1	0	0	0 (10H)	Data (numeric)
1	0	0	0	1	0	1	1 (11H)	"
0	1	0	0	1	0	1	2 (12H)	"
1	1	0	0	1	0	0	3 (13H)	"
0	0	1	0	1	0	1	4 (14H)	"
1	0	1	0	1	0	0	5 (15H)	"
0	1	1	0	1	0	0	6 (16H)	"
1	1	1	0	1	0	1	7 (17H)	"
0	0	0	1	1	0	1	8 (18H)	"
1	0	0	1	1	0	0	9 (19H)	"
0	1	0	1	1	0	0	: (1AH)	Special
1	1	0	1	1	0	1	; (1BH)	"
0	0	1	1	1	0	0	< (1CH)	"
1	0	1	1	1	0	1	= (1DH)	"
0	1	1	1	1	0	1	> (1EH)	"
1	1	1	1	1	0	0	? (1FH)	End Sentinel
0	0	0	0	0	1	0	@ (20H)	Special
1	0	0	0	0	1	1	A (21H)	Data (alpha)
0	1	0	0	0	1	1	B (22H)	"
1	1	0	0	0	1	0	C (23H)	"
0	0	1	0	0	1	1	D (24H)	"
1	0	1	0	0	1	0	E (25H)	"
0	1	1	0	0	1	0	F (26H)	"
1	1	1	0	0	1	1	G (27H)	"
0	0	0	1	0	1	1	H (28H)	"
1	0	0	1	0	1	0	I (29H)	"
0	1	0	1	0	1	0	J (2AH)	"
1	1	0	1	0	1	1	K (2BH)	"
0	0	1	1	0	1	0	L (2CH)	"
1	0	1	1	0	1	1	M (2DH)	"
0	1	1	1	0	1	1	N (2EH)	"
1	1	1	1	0	1	0	O (2FH)	"
0	0	0	0	1	1	1	P (30H)	"
1	0	0	0	1	1	0	Q (31H)	"
0	1	0	0	1	1	0	R (32H)	"
1	1	0	0	1	1	1	S (33H)	"
0	0	1	0	1	1	0	T (34H)	"
1	0	1	0	1	1	1	U (35H)	"
0	1	1	0	1	1	1	V (36H)	"
1	1	1	0	1	1	0	W (37H)	"
0	0	0	1	1	1	0	X (38H)	"
1	0	0	1	1	1	1	Y (39H)	"

0	1	0	1	1	1	1	Z (3AH)	"	
1	1	0	1	1	1	0	[(3BH)	Special	
0	0	1	1	1	1	1	\ (3DH)	Special	
1	0	1	1	1	1	0	] (3EH)	Special	
0	1	1	1	1	1	0	^ (3FH)	Field Separator	
1	1	1	1	1	1	1	_ (40H)	Special	

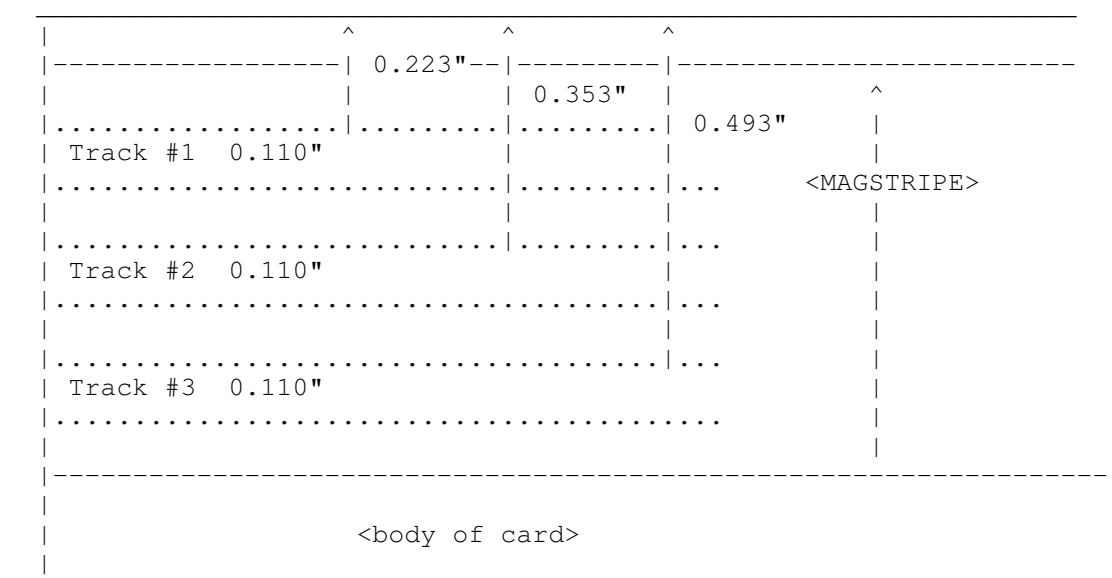
***** 64 Character 7-bit Set *****
* 43 Alphanumeric Data Characters
* 3 Framing/Field Characters
* 18 Control/Special Characters

The two ANSI/ISO formats, ALPHA and BCD, allow a great variety of data to be stored on magstripes. Most cards with magstripes use these formats, but occasionally some do not. More about those later on.

** Tracks and Encoding Protocols **

Now we know how the data is stored. But WHERE is the data stored on the magstripe? ANSI/ISO standards define *3* Tracks, each of which is used for different purposes. These Tracks are defined only by their location on the magstripe, since the magstripe as a whole is magnetically homogeneous. See Figure 8.

Figure 8:



You can see the exact distances of each track from the edge of the card, as well as the uniform width and spacing. Place a magstripe card in front of you with the magstripe visible at the bottom of the card. Data is encoded from left to right (just like reading a book). See Figure 9.

Figure 9:
ANSI/ISO Track 1,2,3 Standards

Track	Name	Density	Format	Characters	Function
1	IATA	210 bpi	ALPHA	79	Read Name & Account
2	ABA	75 bpi	BCD	40	Read Account
3	THRIFT	210 bpi	BCD	107	Read Account & *Encode* Transaction

*** Track 1 Layout: ***

| SS | FC | PAN | Name | FS | Additional Data | ES | LRC |

SS=Start Sentinel "%"
FC=Format Code
PAN=Primary Acct. # (19 digits max)
FS=Field Separator "^"
Name=26 alphanumeric characters max.
Additional Data=Expiration Date, offset, encrypted PIN, etc.
ES=End Sentinel "?"
LRC=Longitudinal Redundancy Check

*** Track 2 Layout: ***

| SS | PAN | FS | Additional Data | ES | LRC |

SS=Start Sentinel ";"
PAN=Primary Acct. # (19 digits max)
FS=Field Separator "="
Additional Data=Expiration Date, offset, encrypted PIN, etc.
ES=End Sentinel "?"
LRC=Longitudinal Redundancy Check

*** Track 3 Layout: ** Similar to tracks 1 and 2. Almost never used.
Many different data standards used.

Track 2, "American Banking Association," (ABA) is most commonly used. This is the track that is read by ATMs and credit card checkers. The ABA designed the specifications of this track and all world banks must abide by it. It contains the cardholder's account, encrypted PIN, plus other discretionary data.

Track 1, named after the "International Air Transport Association," contains the cardholder's name as well as account and other discretionary data. This track is sometimes used by the airlines when securing reservations with a credit card; your name just "pops up" on their machine when they swipe your card!

Since Track 1 can store MUCH more information, credit card companies are trying to urge retailers to buy card readers that read Track 1. The *problem* is that most card readers read either Track 1 or Track 2, but NOT BOTH! And the installed base of readers currently is biased towards Track 2. VISA USA is at the front of this 'exodus' to Track 1, to the point where they are offering Track 1 readers at reduced prices thru participating banks. A spokesperson for VISA commented:

> "We think that Track 1 represents more flexibility and the potential to deliver more information, and we intend to build new services around the increased information."

What new services? We can only wait and see.

Track 3 is unique. It was intended to have data read and WRITTEN on it. Cardholders would have account information UPDATED right on the magstripe. Unfortunately, Track 3 is pretty much an orphaned standard. Its *original* design was to control off-line ATM transactions, but since ATMs are now on-line ALL THE TIME, it's pretty much useless. Plus the fact that retailers and banks would have to install NEW card readers to read that track, and that costs $$.

Encoding protocol specifies that each track must begin and end with a length of all Zero bits, called CLOCKING BITS. These are used to synch the self-clocking feature of biphase decoding. See Figure 10.

Figure 10: end sentinel

```
                    start sentinel      |  longitudinal redundancy check
                      |                 |  |
      000000000000000 SS.................ES LRC 0000000000000000
       leading           data, data, data          trailing
       clocking bits                               clocking bits
       (length varies)                            (length varies)
```

THAT'S IT!!! There you have the ANSI/ISO STANDARDS! Completely explained. Now, the bad news. NOT EVERY CARD USES IT! Credit cards and ATM cards will follow these standards. BUT, there are many other types of cards out there. Security passes, copy machine cards, ID badges, and EACH of them may use a PROPRIETARY density/format/track-location system. ANSI/ISO is REQUIRED for financial transaction cards used in the international interbank network. All other cards can play their own game.

The good news. MOST other cards follow the standards, because it's EASY to follow a standard instead of WORKING to make your OWN! Most magstripe cards other than credit cards and ATM cards will use the same Track specifications, and use either BCD or ALPHA formats.

** A Bit About Magstripe Equipment **

"Wow, now I know how to interpret all that data on magstripes! But.waitasec, what kind of equipment do I need to read the stripes? Where can I buy a reader? I don't see any in Radio Shack!!"

Sorry, but magstripe equipment is hard to come by. For obvious reasons, card readers are not made commonly available to consumers. How to build one is the topic for another file (this file is already too long).

Your best bets are to try and scope out Electronics Surplus Stores and flea markets. Do not even bother trying to buy one directly from a manufacturer, since they will immediately assume you have "criminal motives." And as for getting your hands on a magstripe ENCODER...well, good luck! Those rare beauties are worth their weight in gold. Keep your eyes open and look around, and MAYBE you'll get lucky! A bit of social engineering can go a LONG way.

There are different kinds of magstripe readers/encoders. The most common ones are "swipe" machines: the type you have to physically slide the card thru. Others are "insertion" machines: like ATM machines they 'eat' your card, then regurgitate it after the transaction. Costs are in the thousands of dollars, but like I said, flea markets and surplus stores will often have GREAT deals on these things. Another problem is documentation for these machines. If you call the manufacturer and simply ask for 'em, they will probably deny you the literature. "Hey son, what are you doing with our model XYZ swipe reader? That belongs in the hands of a "qualified" merchant or retailer, not some punk kid trying to "find out how things work!" Again, some social engineering may be required. Tell 'em you're setting up a new business. Tell 'em you're working on a science project. Tell 'em anything that works!

2600 Magazine recently had a good article on how to build a machine that copies magstripe cards. Not much info on the actual data formats and encoding schemes, but the device described is a start. With some modifications, I bet you could route the output to a dumb terminal (or thru a null modem cable) in order to READ the data. Worth checking out the schematics.

As for making your own cards, just paste a length of VCR, reel-to-reel, or audio cassette tape to a cut-out posterboard or plastic card. Works just as good as the real thing, and useful to experiment with if you have no expired or 'dead' ATM or calling cards lying around (SAVE them, don't TOSS them!).

** Examples of Data on Magstripes **

The real fun in experimenting with magstripe technology is READING cards to find out WHAT THE HELL is ON them! Haven't you wondered? The following cards are the result of my own 'research'. Data such as specific account numbers and

names has been changed to protect the innocent. None the cards used to make this list were stolen or acquired illegally.

Notice that I make careful note of "common data." This is data that I noticed was the same for all cards of a particular type. This is highlighted below the data with asterisks (*). Where I found varying data, I indicate it with "x"'s. In those cases, NUMBER of CHARACTERS was consistent (the number of "x"'s equals the number of characters...one to one relationship).

I still don't know what some of the data fields are for, but hopefully I will be following this file with a sequel after I collect more data. It ISN'T easy to find lots of cards to examine. Ask your friends, family, and co-workers to help! "Hey, can I, ahh, like BORROW your MCI calling card tonight? I'm working on an, ahh, EXPERIMENT. Please?" Just...be honest! Also, do some trashing. People will often BEND expired cards in half, then throw them out. Simply bend them back into their normal shape, and they'll usually work (I've done it!). They may be expired, but they're not ERASED!

```
-=Mastercard=-  Number on front of card -> 1111 2222 3333 4444
                Expiration date -> 12/99

Track 2 (BCD,75 bpi)-> ;1111222233334444=99121010000000000000?
                                          ***

Track 1 (ALPHA,210 bpi)-> %B1111222233334444^PUBLIC/JOHN?
                           *
```

Note that the "101" was common to all MC cards checked, as well as the "B".

```
-=VISA=-  Number on front of card -> 1111 2222 3333 4444
          Expiration date -> 12/99

Track 2 (BCD,75 bpi)-> ;1111222233334444=9912101xxxxxxxxxxxxx?
                                          ***
Track 1 (ALPHA,210 bpi)-> %B1111222233334444^PUBLIC/JOHN^9912101xxxxxxxxxxxxx?
                           *
```

Note that the "101" was common to all VISA cards checked, as well as the "B". Also, the "xxx" indicates numeric data that varied from card to card, with no apparent pattern. I believe this is the encrypted pin for use when cardholders get 'cash advances' from ATMs. In every case, tho, I found *13* digits of the stuff.

```
-=Discover=-  Number on front of card -> 1111 2222 3333 4444
              Expiration date -> 12/99

Track 2 (BCD,75 bpi)-> ;1111222233334444=991210100000?
                                          ********

Track 1 (ALPHA,210 bpi)-> %B1111222233334444^PUBLIC/JOHN___^991210100000?
                                                           ********
```

Note, the "10100000" and "B" were common to most DISCOVER cards checked. I found a few that had "10110000" instead. Don't know the significance. Note the underscores after the name JOHN. I found consistently that the name data field had *26* characters. Whatever was left of the field after the name was "padded" with SPACES. So...for all of you with names longer than 25 (exclude the "/") characters, PREPARE to be TRUNCATED! ;)

```
-=US Sprint FON=-  Number on front of card -> 111 222 3333 4444

Track 2 (BCD,75 bpi)-> ;xxxxxx11122233339==xxx4444xxxxxxxxxx=?
                                       *

Track 1 (ALPHA,210 bpi)-> %B^ /^^xxxxxxxxxxxxxxxx?
                           *
```

Strange. None of the cards I check had names in the Track 1 fields. Track 1 looks unused, yet it was always formatted with field separators. The "xxx" stuff varied from card to card, and I didn't see a pattern. I know it isn't

a PIN, so it must be account data.

-=Fleet Bank=- Number on front of card -> 111111 222 3333333
Expiration date -> 12/99

Track 2 (BCD,75 bpi)-> ;1111112223333333=9912120100000000xxxx?
****

Track 1 (ALPHA,210 bpi) ->
%B1111112223333333^PUBLIC/JOHN___^99121201000000000000xxxx000000?
* ****

Note that the "xxx" data varied. This is the encrypted PIN offset. Always 4 digits (hmmm...). The "1201" was always the same. In fact, I tried many ATM cards from DIFFERENT BANKS...and they all had "1201".

(Can't leave *this* one out ;)
-=Radio Shack=- Number on front of card -> 1111 222 333333
NO EXPIRATION data on card

Track 2 (BCD,75 dpi)-> ;1111222333333=9912101?
****

Note that the "9912101" was the SAME for EVERY Radio Shack card I saw. Looks like when they don't have 'real' data to put in the expiration date field, they have to stick SOMETHING in there.

Well, that's all I'm going to put out right now. As you can see, the major types of cards (ATMs, CC) all follow the same rules more or less. I checked out a number of security passcards and timeclock entry cards..and they ALL had random stuff written to Track 2. Track 2 is by FAR the MOST utilized track on the card. And the format is pretty much always ANSI/ISO BCD. I *did* run into some hotel room access cards that, when scanned, were GARBLED. They most likely used a character set other than ASCII (if they were audio tones, my reader would have put out NOTHING...as opposed to GARBLED data). As you can see, one could write a BOOK listing different types of card data. I intended only to give you some examples. My research has been limited, but I tried to make logical conclusions based on the data I received.

** Cards of All Flavors **

People wanted to store A LOT of data on plastic cards. And they wanted that data to be 'invisible' to cardholders. Here are the different card technologies that were invented and are available today.

HOLLERITH - With this system, holes are punched in a plastic or paper card and read optically. One of the earliest technologies, it is now seen as an encoded room key in hotels. The technology is not secure, but cards are cheap to make.

BAR CODE - The use of bar codes is limited. They are cheap, but there is virtually no security and the bar code strip can be easily damaged.

INFRARED - Not in widespread use, cards are factory encoded by creating a "shadow pattern" within the card. The card is passed thru a swipe or insertion reader that uses an infrared scanner. Infrared card pricing is moderate to expensive, and encoding is pretty secure. Infrared scanners are optical and therefore vulnerable to contamination.

PROXIMITY - Hands-free operation is the primary selling point of this card. Although several different circuit designs are used, all proximity cards permit the transmission of a code simply by bringing the card near the reader (6-12"). These cards are quite thick, up to 0.15" (the ABA standard is 0.030"!).

WIEGAND - Named after its inventor, this technology uses a series of small diameter wires that, when subjected to a changing magnetic field, induce a discrete voltage output in a sensing coil. Two rows of wires are embedded in a coded strip. When the wires move past the read head, a series of pulses is read and interpreted as binary code. This technology produces cards that are VERY hard to copy or alter, and cards are moderately expensive to make. Readers based on this tech are epoxy filled, making them immune to weather conditions, and neither card nor readers are affected by external magnetic fields (don't worry about leaving these cards on top of the television set...you can't hurt them!). Here's an example of the layout of the wires in a Wiegand strip:

```
   ||| || ||   | ||| | || ||    |  ||  ||    |   |  ||
      |  |    | |   | |     ||||     ||  ||||     ||
```

The wires are NOT visible from the outside of the card, but if your card is white, place it in front of a VERY bright light source and peer inside. Notice that the spacings between the wires is uniform.

BARIUM FERRITE - The oldest magnetic encoding technology (been around for 40 yrs!) it uses small bits of magnetized barium ferrite that are placed inside a plastic card. The polarity and location of the "spots" determines the coding. These cards have a short life cycle, and are used EXTENSIVELY in parking lots (high turnover rate, minimal security). Barium Ferrite cards are ONLY used with INSERTION readers.

There you have the most commonly used cards. Magstripes are common because they are CHEAP and relatively secure.

** Magstripe Coercivity **

Magstripes themselves come in different flavors. The COERCIVITY of the magnetic media must be specified. The coercivity is the magnetic field strength required to demagnetize an encoded stripe, and therefore determines the encode head field strength required to encode the stripe. A range of media coercivities are available ranging from 300 Oersteds to 4,000 Oe. That boils down to HIGH-ENERGY magstripes (4,000 Oe) and LOW-ENERGY magstripes (300 Oe).

REMEMBER: since all magstripes have the same magnetic remanence regardless of their coercivity, readers CANNOT tell the difference between HIGH and LOW energy stripes. Both are read the same by the same machines.

LOW-ENERGY media is most common. It is used on all financial cards, but its disadvantage is that it is subject to accidental demagnetization from contact with common magnets (refrigerator, TV magnetic fields, etc.). But these cards are kept safe in wallets and purses most of the time.

HIGH-ENERGY media is used for ID Badges and access control cards, which are commonly used in 'hostile' environments (worn on uniform, used in stockrooms). Normal magnets will not affect these cards, and low-energy encoders cannot write to them.

** Not All that Fluxes is Digital **

Not all magstripe cards operate on a digital encoding method. SOME cards encode AUDIO TONES, as opposed to digital data. These cards are usually used with old, outdated, industrial-strength equipment where security is not an issue and not a great deal of data need be encoded on the card. Some subway passes are like this. They require only expiration data on the magstripe, and a short series of varying frequencies and durations are enough. Frequencies will vary with the speed of swiping, but RELATIVE frequencies will remain the same (for instance, tone 1 is twice the freq. of tone 2, and .5 the freq of tone 3, regardless of the original frequencies!). Grab an oscilloscope to

visualize the tones, and listen to them on your stereo. I haven't experimented with these types of cards at all.

** Security and Smartcards **

Many security systems utilize magstripe cards, in the form of passcards and ID cards. It's interesting, but I found in a NUMBER of cases that there was a serious FLAW in the security of the system. In these cases, there was a code number PRINTED on the card. When scanned, I found this number encoded on the magstripe. Problem was, the CODE NUMBER was ALL I found on the magstripe! Meaning, by just looking at the face of the card, I immediately knew exactly what was encoded on it. Ooops! Makes it pretty damn easy to just glance at Joe's card during lunch, then go home and pop out my OWN copy of Joe's access card! Fortunately, I found this flaw only in 'smaller' companies (sometimes even universities). Bigger companies seem to know better, and DON'T print ALL of the magstripe data right on card in big, easily legible numbers. At least the big companies *I* checked. ;)

Other security blunders include passcard magstripes encoded ONLY with the owner's social security number (yeah, real difficult to find out a person's SS#...GREAT idea), and having passcards with only 3 or 4 digit codes.

Smartcard technology involves the use of chips embedded in plastic cards, with pinouts that temporarily contact the card reader equipment. Obviously, a GREAT deal of data could be stored in this way, and unauthorized duplication would be very difficulty. Interestingly enough, not much effort is being put into smartcards by the major credit card companies. They feel that the tech is too expensive, and that still more data can be squeezed onto magstripe cards in the future (especially Track 1). I find this somewhat analogous to the use of metallic oxide disk media. Sure, it's not the greatest (compared to erasable-writable optical disks), but it's CHEAP..and we just keep improving it. Magstripes will be around for a long time to come. The media will be refined, and data density increased. But for conventional applications, the vast storage capabilities of smartcards are just not needed.

** Biometrics: Throw yer cards away! **

I'd like to end with a mention of biometrics: the technology based on reading the physical attributes of an individual thru retina scanning, signature verification, voice verification, and other means. This was once limited to government use and to supersensitive installations. However, biometrics will soon acquire a larger market share in access control sales because much of its development stage has passed and costs will be within reach of more buyers. Eventually, we can expect biometrics to replace pretty much ALL cards..because all those plastic cards in your wallet are there JUST to help COMPANIES *identify* YOU. And with biometrics, they'll know you without having to read cards.

I'm not paranoid, nor do I subscribe to any grand "corporate conspiracy," but I find it a bit unsettling that our physical attributes will most likely someday be sitting in the cool, vast electronic databases of the CORPORATE world. Accessible by anyone willing to pay. Imagine CBI and TRW databases with your retina image, fingerprint, and voice pattern online for instant, convenient retrieval. Today, a person can CHOOSE NOT to own a credit card or a bank card...we can cut up our plastic ID cards! Without a card, a card reader is useless and cannot identify you.

Paying in cash makes you invisible! However, with biometrics, all a machine has to do is watch... listen...and record. With government/corporate America pushing all the buttons. "Are you paying in cash?..Thank you...Please look into the camera. Oh, I see your name is Mr. Smith...uh, oh...my computer tells me you haven't paid your gas bill...afraid I'm going to have to keep this money and credit your gas account with it....do you have any more cash?...or would you rather I garnish your paycheck?" heh heh

** Closing Notes (FINALLY!!!!) **

Whew...this was one MOTHER of a file. I hope it was interesting, and I hope you distribute it to all you friends. This file was a production of "Restricted Data Transmissions"...a group of techies based in the Boston area that feel that "Information is Power"...and we intend to release a number of highly technical yet entertaining files in the coming year....LOOK FOR THEM!! Tomorrow I'm on my way to Xmascon '91... we made some slick buttons commemorating the event...if you ever see one of them (green wreath.XMASCON 1991 printed on it).hang on to it!... it's a collector's item.. (hahahah) Boy, I'm sleepy...

Remember.... "Truth is cheap, but information costs!"

But -=RDT is gonna change all that... ;) set the info FREE!

Peace.

..oooOO Count Zero OOooo..

Usual greets to Magic Man, Brian Oblivion, Omega, White Knight, and anyone else I ever bummed a cigarette off.

(1/18/92 addition: Greets to everyone I met at Xmascon..including but not excluding Crimson Death, Dispater, Sterling, Mack Hammer, Erik Bloodaxe, Holistic Hacker, Pain Hertz, Swamp Ratte, G.A.Ellsworth, Phaedrus, Moebius, Lord MacDuff, Judge Dredd, and of course hats off to *Drunkfux* for organizing and taking responsibility for the whole damn thing. Hope to see all of you at SummerCon '92! Look for Cyber-striper GIFs at a BBS near you..heh heh)

Comments, criticisms, and discussions about this file are welcome. I can be reached at:

count0@world.std.com
count0@spica.bu.edu
count0@atdt.org

Magic Man and I are the sysops of the BBS "ATDT"...located somewhere in Massachusetts. Great message bases, technical discussions...data made flesh...electronic underground.....our own Internet address (atdt.org)... field trips to the tunnels under MIT in Cambridge.....give it a call.. mail me for more info.. ;)

```
      <:=-=:><:=-=:><:=-=:><:=-=:>\|/<:=-=:><:=-=:><:=-=:><:=-=:>
      <:=-=:>                                                   <:=-=:>
      <:=-=:>    >>>>>=-*  Users Guide to VAX/VMS  *-=<<<<<     <:=-=:>
      <:=-=:>                                                   <:=-=:>
      <:=-=:>                   Part II of III                  <:=-=:>
      <:=-=:>                                                   <:=-=:>
      <:=-=:>            Part C: Using the Utilities            <:=-=:>
      <:=-=:>         Part D: Advanced Guide to VAX/VMS         <:=-=:>
      <:=-=:>                                                   <:=-=:>
      <:=-=:>                    By Black Kat                   <:=-=:>
      <:=-=:>                                                   <:=-=:>
      <:=-=:><:=-=:><:=-=:><:=-=:>/|\<:=-=:><:=-=:><:=-=:><:=-=:>
```

Index

Part C contains information on the following topics:

- Help Utility
- Backup Utility
- Mail Utility
- Phone Utility
- Library Utility
- Sort Utility

Part D contains information on the following topics:

- Subprocesses
- Attaching to a Process
- Interrupting a Process
- Batch Processing
- Controlling Batch Jobs
- DECnet
- Proxy Access
- Task-to-Task Communication
- Remote Printing
- VAXclusters

<:=- Part C : Using the Utilities -=:>

Help Utility

The VAX/VMS Help Utility is almost like having a DCL dictionary online. It includes an explanation of each DCL command and can optionally explain valid command parameters. Help also provides information about other VAX/VMS utilities and system services.

There are two modes available for the help utility. If you know the DCL command, utility or system service you want more information about, use direct mode. If you don't know the command, use query mode. Query mode can also be used to see which other commands and other subjects are referenced by the help utility.

To use query mode, just type HELP <enter> at the DCL command level. Help will display an alphabetical listing of all DCL commands and other topics for which information is available and you will be prompted with: "Topic?"

You can exit Help by pressing <enter> or <Ctrl-C> or <Ctrl-Z> or get information by typing in the command or subject name followed by <enter>. When you request information on a command, Help will display details including how the command is invoked, what it does and the default values. Most topics will have subtopics available which will be listed alphabetically followed by the prompt: "COMMAND-NAME Subtopic?"

You can select subtopic help or press <enter> to return to the "Topic?" prompt. If you want to see all the information available on a command, type in "HELP command_name ..." or "HELP command_name *".

To use direct mode, enter HELP topic_name <enter>. This will bypass the listing of available topic. Additionally, you can enter a valid DCL command with or without qualifiers in this mode. For example, to get information on the DCL SET command /TERMINAL qualifier, you could enter $ HELP SET TERMINAL. The help utility will provide information on the SET/TERMINAL command and prompt you for another subtopic since information on other qualifiers is available.

For more information and details on the help utility, you can use:

$ HELP HINTS or $ HELP HELP/INSTRUCTIONS.

Backup Utility

The backup utility is usually used by system managers to back up system disks, insuring a recent copy of data should the system disks become unreliable. Generally, the system disks are backed up to magnetic tape or removable disk packs, which are then removed and stored in a save location offline. Users may use the backup utility on files in their own accounts to make copies for safe keeping, transferring to another system, or for offline storage.

To use the backup utility, you have to decide what you want to back up, and how you want it done. You have the following options:

```
Selective   :  Files are backed up according to a specified criteria.
               Qualifiers (e.g. /DATE) and file specifications (e.g. *.TXT)
               are used for specifying these criteria.
File by File:  Individual files or entire file directories are backed up.
               Directories are created when copying, unlike the copy command.
Incremental :  Saves file created since the most recent backup.  Usually
               performed by system operators.
Physical    :  An exact duplicate of a volume is saved.  All file structures
               are ignored and the copy is a bit-by-bit duplicate.
Image       :  A functionally equivalent copy of the original volume is
               created.  Typically done on bootable volumes and system disks.
```

To back up files to a subdirectory: $ BACKUP F1.TXT,F2.TXT,*.DAT [BY.JUNK]

To copy a directory tree: $ BACKUP [dir...]file_spec [dir...]file_spec

To copy disk volumes:

```
$ MOUNT/FOREIGN DJA1:
$ BACKUP/IMAGE DUA2: DUA1:
```

To copy to tape:

```
$ INITIALIXE MUA0: TAPE  (the first time its used)
$ MOUNT/FOREIGH MUA0:
   MOUNT-I-MOUNTED, TAPE mounted on __MUA0:
$ BACKUP [.DRV]MV_DYDRV.MAR MUA0:[]MV_DYDRV.MAR
```

A save set is a single file containing multiple files that have been backed up. To make a save set:

```
$ MOUNT/FOREIGN MUA0:
   MOUNT-I-MOUNTED, TAPE mounted on __MUA0:
$ BACKUP DUB1:[BY.JUNK]*.*;* MUA0:08JUN.BAK/SAVE_SET
```

A single file can be retrieved from a save set by using the /SELECT qualifier. For example, to restore the file LOGIN.COM from the previously backed up save set:

```
$ MOUNT/FOREIGH MUA0:
   MOUNT-I-MOUNTED, TAPE mounted on __MUA0:
$ BACKUP
__From: MUA0:08:JUN.BAK/SAVE_SET/SELECT=[BY.JUNK]LOGIN.COM
__To: *.*
```

Listing a save set:

```
$ MOUNT/FOREIGN MUA0:
   MOUNT-I-MOUNTED, TAPE mounted on __MUA0:
$ BACKUP/LIST MUA0:08JUN.BAK/SAVE_SET
```

Selective backups:

```
$ BACKUP *.*/SINCE=12-APR-1988 MUA0:08JUN.BAK/SAVE_SET
$ BACKUP
__From: *.*/SINCE=12-APR-1988/EXCLUDE=[*.TMP,*.LOG]
__To: MUA0:08JUN.BAK/SAVE_SET
```

The following is a list of some other qualifiers you'll find useful.

Qualifier	Function
/LOG	Writes log message to terminal as each backup file is written.
/VERIFY	Verifies the copy or save set with the original after copy.
/CONFIRM	Display each filename and ask for confirmation before copy.
/DELETE	Deletes source file after destination file written.

Mail Utility

When you receive new mail, a message will be sent to your terminal unless the /NOBROATCAST qualifier has been specified with the SET TERMINAL command. Mail is an interactive utility that understands many commands in a format identical to DCL commands. The utility is invoked by typing "$ MAIL" at the DCL command level. Mail has a built in help feature which works the same way as the VAX/VMS Help Utility. Mail may be sent interactively or directly.

Interactive implies the use of the mail utility in conversational mode by invoking mail at the DCL command level. After invoking the mail utility, use the SEND command, and mail will prompt you for the name of the user(s) you want to send the mail to, your name, the subject, and the message text which you will terminate with <Ctrl-Z>. When you press <Ctrl-Z> the message is sent and you are returned to the mail prompt where you can type EXIT to quit.

To send mail in direct mode from the DCL command line, use the following format: $ MAIL file_spec user /SUBJECT="character string" where "file_spec" is a valid VAX/VMS file specification containing the body of your mail message and "user" is the name of a user on your local system or remote node. The /SUBJECT qualifier is optional.

To send mail to multiple users (like a mailing list) create a file with a list of the account names of every user you want to receive the message. Then enter @FILENAME at the "To:" prompt and each user listed in the distribution list will receive a copy of your mail. A distribution list may also contain another distribution list by preceeding the second name with an at sign (@). Comments are included by using an exclamation point (!). The following is a sample distribution list:

```
! VAX.DIS
!
! Staff
JONES
OPER
BYNON
!
! Accounting personnel
@ACTLIST
```

To read your mail, just type MAIL <enter> and you will be told how many messages you have waiting. Read is the default command, so you can just press <enter> to start reading them. To reply to a message, use the REPLY or ANSWER commands and the mail utility will fill out the header information automatically. You can store your mail in folders for later reference. The system has three default folders (MAIL, NEWMAIL, and WASTEBASKET).

MAIL is the default mail folder and always exists. It is used to store mail messages after you've read them unless you file these messages in other folders you've created.

The NEWMAIL folder stores mail messages before you read them, like a mailbox. They're automatically moved to the MAIL folder after you've read them unless you specify a different destination folder with the MOVE command.

The WASTEBASKET folder is a temporary folder used to store messages that have been deleted. These messages remain in the WASTEBASKET folder until you exit the mail utility, at which time they're thrown out permanently.

To create new folders, select a message and enter the MOVE command. If you attempt to move a message to a nonexistent folder, you'll be asked if you want to create a new folder. For example:

```
MAIL> 11
MAIL> MOVE MEMOS
Folder MEMOS does not exist. Create it (Y/N, default is N)? Y
MAIL-NEWFOLDER, folder MEMOS created MAIL>
```

The SELECT command allows you to move from one folder to another. For example, if you type SELECT JUNK at the "MAIL>" prompt, you will be moved to the JUNK folder, and mail will respond with the number of messages contained in the new folder.

The DELETE command accepts a message number as a parameter or deletes the current message if a message number is not supplied. To delete a folder, just delete all the messages in that folder with the DELETE qualifier /ALL.

To log a mail message to a file, use the EXTRACT qualifier. If the /NOHEADER qualifier is used, the header information will not be included. For example: EXTRACT/NOHEADER MEMO.TXT will save the currently selected message to a file named MEMO.TXT.

For more information on the mail utility, use mail's HELP command.

Phone Utility

The VAX/VMS Phone Utility allows you to talk to other users on your system. It simulates a real telephone with such features as call holding, conference calls and telephone directories. The Phone utility only works with VT100, VT200 or compatible terminals.

To call someone with the phone utility, enter "$ PHONE username" where username is the person you want to talk to. Your screen will split horizontally in half and indicate that the phone utility is ringing the other person. Your half of the conversation will be displayed on the top of the screen and the other person's will appear on the lower half.

The phone utility may also be used interactively by entering "$ PHONE", and you will now be given the phone prompt (%). You can enter commands directly now (e.g. "% DIRECTORY"). The phone utility has an online help facility just like the mail utility.

Library Utility

Sometimes its easier to maintain a single file instead of a group of related files. The VAX/VMS Library Utility lets you create and maintain a specially formatted file called a library in which you can store groups of single files called modules. Predefined libraries include text, help, object, sharable image and macro. Many VAX/VMS utilities such as HELP and LINK are capable of processing library files. Unless you're a programmer or system manager, you'll probably only use text and help libraries.

To create a library use the LIBRARY command's /type qualifier and the /CREATE qualifier. The /type qualifiers are: /TEXT, /SHARE, /HELP, /OBJECT, /MACRO. For example to create a text library named BOOK.TLB:

```
$ LIBRARY/TEXT/CREATE BOOK.
```

You may optionally specify a list of files to be included in a library when it is created. For example:

```
$ LIBRARY/TEXT/CREATE BOOK TOC,C1,C2,INDEX
```

To list the names of modules in a library, use the /LIST qualifier:

```
$ LIBRARY/TEXT/LIST BOOK
Directory of TEXT library BOOK.TLB;1 on 12-JUN-1989 14:12:07
TOC
C1
C2
INDEX
```

You can also display a history of updates made to the library by using the /HISTORY qualifier with the /LIST qualifier.

To add modules to an existing library, use the /INSERT qualifier:

```
$ LIBRARY/TEXT/INSERT BOOK CH3
```

To update a module in a library, do the following:

- Extract the module to be updated with the /EXTRACT qualifier.
- Make the necessary changes.
- Write over the old module with the /REPLACE qualifier.

```
For example:  $ LIBRARY/TEXT/EXTRACT BOOK CH2
              $ EDIT CHAP2.TXT
                .
                .    (edit the file)
                .
              $ LIBRARY/TEXT/REPLACE BOOK CH2
```

Sort Utility

The VAX/VMS Sort Utility will reorganize records within a file. The simplest form of the sort command will organize records in ascending alphabetical order. For example, to sort BOOK.TXT, you could issue the command:

```
$ SORT BOOK.TXT SORTED.TXT
```

The Sort utility sorts on the first character of the field in each record in the input file. If there is more than one field or column in a record, the entire record is ordered, not just the first field.

Here's an example of sorting in descending order numerically with multiple fields. The sample data file JUNK.TXT contains two fields of data. The first field contains a name, and the second field, starting in column 9 contains the two-digit number we're sorting by:

```
PAT     47
PAT     47
JIM     09
TOM     23
RICH    43
GARY    02
KURT    13
KEVIN   27
```

Sort the file: `$ SORT/KEY=(POSITION=9,SIZE=2,DESCENDING) JUNK.TXT SORTED.TXT`

The sorted file (SORTED.TXT) will now look like this:

```
PAT     47
RICH    43
KEVIN   27
TOM     23
KURT    13
JIM     09
GARY    02
```

Subprocesses

A major benefit of the VAX/VMS operating system is its support of multi-processing. This is not restricted to multiple users logged into different terminals however. VAX/VMS users may create multiple processes known as subprocesses from within their main processes.

The DCL SPAWN command is used to create a subprocess. The SPAWN command will create a subprocess with the attributes (default directory, privileges, memory, etc.) of its parent process unless otherwise specified. For example:

```
$ SPAWN
% DCL-S-SPAWNED, process BYNON_1 spawned
% DCL-S-ATTACHED, terminal now attached to process BYNON_1
```

In this case, the parent process is put into hibernation, the subprocess is given control of the keyboard, and we are left at the DCL prompt. You can now enter any DCL commands, utilities, or other programs. To return to the parent process, just $ LOGOUT of the subprocess:

```
$ LOGOUT
  Process BYNON_1 logged out at 12-JUL-1981 13:04:17.10
$ DCL-S-RETURNED, control returned to process BYNON
```

The SPAWN qualifier /NOLOG can be used to suppress the informational messages generated when a subprocess is created or logged out. DCL Commands, procedures and VAX/VMS images (utilities and programs) may be executed directly with SPAWN by entering the correct syntax for the command or procedure after the SPAWN command. For example: $ SPAWN/NOLOG MAIL

If you have a task that can execute without user intervention (e.g. a program compiler), you can spawn a task to run as a background process to your current process. For example: $ SPAWN/NOWAIT FORTRAN VAXBBS

The SPAWN qualifier /NOWAIT spawns the task to run concurrently (parallel) to the parent process. Both processes will share the terminal and any messages >from the background task will be displayed at the terminal. To avoid possible conflicts, use the /OUTPUT qualifier:

```
$ SPAWN/NOWAIT/OUTPUT=COMPILE.LOG FORTRAN.VAXBBS
```

When the job in the subprocess is complete it will terminate and be removed >from the system.

ATTACHing to a Process

You can use the DCL ATTACH command to connect your keyboard to any process or subprocess you've created. To exit from BYNON_1 back to BYNON with the ATTACH command, enter "$ ATTACH BYNON" and the subprocess hibernates while you are returned to the parent process.

Interrupting a Process

You can interrupt a process at anytime to create a subprocess by pressing <Ctrl-Y> and then using the SPAWN command. When you're done working with the subprocess and have returned to the interrupted process, type CONTINUE to start processing again where you left off. Some VAX/VMS utilities, such as MAIL, support SPAWN intrinsically, so you can spawn a process within these utilities by entering the SPAWN command without pressing <Ctrl-Y> first.

Batch Processing

The SUBMIT command was briefly discussed in Part II: Programming the VAX. A batch job is one or more DCL command procedures that execute from a detached

process with your privileges and quotas. The controller of the process is the batch queue which accepts jobs via the SUBMIT command. Batch jobs execute without user interaction, permitting you to use your terminal for interactive work while the system executes the batch job (command procedure). Batch jobs are used to execute tasks that take a long time to run, use many system resources, or need to be scheduled to execute at a specific time.

The SUBMIT command will enter a command procedure to the default batch queue (SYS$BATCH) if a specific queue is not provided. A command procedure submitted for batch execution is given a job name which defaults to the command procedure name unless otherwise specified. The entry number given to the job is used to control it (delete, rename, etc.)

Controlling Batch Jobs

You can specify a name for a batch job with the /NAME qualifier:

```
$ SUBMIT BACKUP /NAME=DAILY_BACK
```

You may also execute more than one command procedure by separating the procedure names with a comma:

```
$ SUMBIT SORT_DATA,REPORT /NAME=WEEKLY_REPORT
```

To schedule a batch job to execute after a specific time:

```
$ SUMBIT CLEANUP /AFTER=11:40
Job CLEANUP (queue SYS$BATCH, entry 39) holding until 1-JUN-1989 11:40
```

To hold a job in the queue to be released later:

```
$ SUMBIT REMINDER /HOLD
Job REMINDER (queue SYS$BATCH, entry 12) holding
$
$ SET QUEUE/ENTRY=32/RELEASE SYS$BATCH
```

To submit a job to a different queue: $ SUBMIT TESTJOB /QUEUE=SLOW

To lower the priority (e.g. if it’s CPU intensive):

```
$ SUBMIT CRUNCH /PRIORITY=2
```

To pass parameters: $ SUBMIT COMPILE / PARAMETERS=(WINDOWS,MISC,DISP_IO)

To disable the automatic printing of the batch job’s log (file instead):

```
$ SUBMIT GOJOB /NOPRINT /LOG_FILE=DUA2:[BYNON]
```

This will create a file DUA2:[BYNON]GOJOB.LOG. If the /NOPRINT qualifier is not specified, the log file will be printed and deleted. To print and keep the log file, use the /KEEP qualifier with the /LOG_FILE qualifier.

After you submit a procedure to a batch queue, you can monitor its status and job characteristics by using the SHOW QUEUE command. This will display the name, entry number and status of all the jobs you have in queue. The /ALL qualifier will display all jobs you have enough privilege to see, and the /FULL qualifier provides more information about jobs, such as operating characteristics and submission time.

You can use the SET QUEUE/ENTRY command to modify a job’s priority (/PRIORITY), name (/NAME), or status (/RELEASE or /AFTER). For example:

```
$ SET QUEUE /ENTRY=217 /PRIORITY=2 SYS$BATCH
```

Use the DELETE /ENTRY command to delete jobs: $ DELETE /ENTRY=18 SYS$BATCH

Using DECnet

DECnet uses the standard VAX/VMS file specifications for remote file access. In addition to a node specification, you may also include access control information (username and password) in quotes. For example:

```
    BURG"JONES MYPW"::DUA2:JUNK.TXT
     |     |    |       |     |
     |     |    |       |     +---- Filename.Extension
     |     |    |       |
     |     |    |       +---------- Device name
     |     |    |
     |     |    +------------------ Password
     |     |
     |     +----------------------- Username
     |
     +--------------------------- Node name
```

Unless a specific DECnet account exists on the host node, or proxy exists, you must supply access control information to execute a command on a remote system. (e.g. $ TYPE BURG""JONES MYPW"::DUA2:JUNK.TXT)

Proxy Access

Because including access control information in a command string is a security risk, Digital provides proxy access, which works by keeping a database of users and hosts who may gain access to the system via DECnet. The format of the database is: SYSTEM::REMOTE_USERNAME LOCAL_USERNAME.

Task-to-Task Communication

This is a feature of DECnet which allows programs on one system to communicate with programs on another (e.g. the DCL TYPE command) To execute a procedure on a remote system, use the TYPE command with the TASK=xxx parameter. For example:

```
$ TYPE VAX1::"TASK=SHOW_USERS"
```

To show the users on a remote system you would write a command procedure something like this:

```
$! Show_Users.Com
$!
$      IF FMODE() .EQS. "NETWORK" THEN GOTO NETWORK
$      SHOW USERS
$      EXIT
$  NETWORK:
$      DEFINE/USER_MODE SYS$OUTPUT SYS$NET
$      SHOW USERS
$      EXIT
```

Since SYS$OUTPUT is redirected to SYS$NET, the output is redirected to your terminal over DECnet. Task-to-Task communication can be simple (like Show_Users) or complicated (like programs passing data back and forth).

Remote Printing

If your DECnet network contains a LAN such as Ethernet, you'll probably have to share printers with other nodes on the network. The easiest way to print a file is to copy it directly to the print device. This works fine as long as the device is spooled and set up with world write privileges. For example: $ COPY JUNK.TXT BURG::LCA0: will copy the file JUNK.TXT to the device LCA0: on node BURG.

Another way to print is to use the DCL PRINT/REMOTE command. However, the file

must be located on the remote system to use this, which is inconvenient if the file you're printing is on the local system. You can still do it though:

```
$ COPY JUNK.TXT BURG::[BYNON]
$ PRINT /REMOTE BURG::[BYNON]JUNK.TXT
   Job JUNK (queue SYS$PRINT, entry 512) started on LCA0
$ DELETE BURG::[BYNON]JUNK.TXT
```

VAXclusters

The main purpose of a VAXcluster is high processor ability, shared resources, and a single security and management area. There are two basic type of VAXclusters, heterogeneous and homogeneous, but a mix of the two is possible. The main difference between these types is how they share resources, specifically the VAX/VMS OS environment.

The VAX/VMS OS environment is identical on each cluster in a homogeneous VAXcluster. This is done by using a common system disk for all the nodes. User accounts, system files, queues and storage devices are shared, and all of the computers behave the same way.

In a heterogeneous VAXcluster, the environment on each system is different. Each VAX has its own system disk, user accounts and system files. Queues and storage devices may or may not be shared. Users can work in different operating environments, depending on the system they're using.

Usually a VAXcluster is accessed by an Ethernet-based terminal server. Using a terminal server, a user can establish a session with any VAXcluster member, and the connection is identical to that of a directly connected terminal. However, terminal sessions can support multiple simultaneous sessions to different nodes. In the unlikely event that a VAXcluster is set up with directly connected terminals and you need to access a different system, you can DECnet via the SET HOST facility. All VAXcluster systems support DECnet within the cluster.

VAXcluster members (nodes) often share processing resources through the use of print and batch queues known as cluster-wide queues, which are used the same as a normal queue. The only extra information you need is the queue name. A list of all the queues in a cluster can be called up with the DCL SHOW QUEUE command. If you submit a job to a cluster-wide queue, you must insure that the node on which it resides has access to the file you want to print or the command procedure you want processed.

Volume Four, Issue Thirty-Seven, File 8 of 14

```
##############################
#*#     Basic Commands     #*#
#*#      for the VOS       #*#
#*#         System         #*#
##############################
```

Written by Dr. No-Good
[Echo]

Introduction

Ok, well this is a simple text file that explains the basic commands used by a VOS system. VOS stands for Virtual Operating System and it is mainly used by businesses but other groups have used it too.

If you have any questions, you can reach me at this fine system:

Legion (202)337=2844

or if you have any questions you can e-mail the me at:

Internet: ukelele!kclahan@UUNET.UU.NET

Special Thanks to: Nat X, Beta Raider, Tomellicus and the anonymous site of my humble work.

$Note$

All material in this t-file is for informational purposes only. Any abuse of this information is probably against the law and the authors of this text file are not responsible for the reader's actions.

(***)

Ok, well VOS systems can be found in various systems around the world and on many of the nets such as TELENET. You can recognize a VOS system at its prompt. Which looks like this:

```
Prompt->     (Name of System)
             System ???, VOS Release v.(version), Module ???

             (Or it just says something about a Release ver# and Module#)
```

After getting the log-on message you come to the hard part, getting a valid user/password combination. To log-in, you type:

```
             Login <name> <password> <CRT>
     or
             Login <CRT>
             'User_name:' <name>
             'Password?' <password>
```

(by the way, <CRT> means enter and it comes after something you have to type and words in '' mean that the computer is displaying that)

When you get a valid name and password, it will say:

<name> logged in on <module#> at <year>-<month>-<day> at <time> ETA.

(then it runs start_up.cm)

(***)

Commands

```
  HELP                       =  To get an on-line help directory.

  LIST or LS                 =  To list contents of the directory.
            -dirs            =          the subdirectories.
            -dirs <dir>      =  To confirm a directory exists.

  CHANGE_CURRENT_DIR or CCD  =  To change directory.

  DISPLAY <file>             =  To view the contents of a file.
            -match <string>  =  To find a string in the file.

  SEND_MESSAGE <name> <msg>  =  To make a message appear on the receiver's
                                   screen.  It must be 80 chars. or less.

  CALL_THRU                  =  To connect your login terminal to a remote
                                   host as a login terminal or as a slave.

  SET_TERMINAL_PARAMETERS    =  To define the operating features of your
                                   terminal such as scrolling, length, etc.

  LOCATE_FILES <file names>  =  To find the location of file(s) in the system.

  WHO                        =  To list the current users of the system.

  LIST_MODULES               =  To show which modules are running.

  DISPLAY_DIR_STATUS         =  It gives information about when last saved,
                                   when it was created, who created, and when
                                   it was last used or modified.

  DISPLAY_CURRENT_DIR        =  It shows you which directory you are in.

  DISPLAY_ACCESS_LIST        =  To show you the access control lists(ACL) for
                                   a set of files or directories.

  DISPLAY_DEFAULT_ACCESS      =  To display the default access control list for
                                   a set of directories you specify.

  GIVE_ACCESS                =  To give a user/group access to a file or
                                   directory.

  GIVE_DEFAULT_ACCESS        =  To add entries to the default ACL or a
                                   directory or set of directories.

  PROPAGATE_ACCESS           =  To copy a directory(DIR)'s access to all the
                                   directories in the subhierarchy.

  REMOVE_ACCESS              =  To remove entries from the ACL of a file or
                                   directory, or a set of such objects.

  REMOVE_DEFAULT_ACCESS      =  To remove entries from the default ACL of a
                                   directory or a set of directories.

  EDIT                       =  To edit or create a file.
                                   (We haven't been able to figure it out yet)

  BIND                       =  To make an .OBJ file a .PM which can be run.

  ANY_NAME.PM                =  .PM stands for program module and it is like a
                                   .COM or .EXE executable file.

  BATCH                      =  To run a batch of .PM commands.

  UPDATE_BATCH_REQUESTS      =  To update the batch queue.

  CANCEL_BATCH_REQUESTS      =  To totally cancel all programs in the batch
                                   queue.
```

```
  LIST_BATCH_REQUESTS       =  To list the programs in the batch queue.

  RESERVE_DEVICE            =  To reserve a device for the batch queue.
                               (Used by administrators when they manage
                                batch processing at a site)

  CANCEL_DEVICE_RESERVATION =  To cancel the device reservation.

  MOVE_DEVICE_RESERVATION   =  To move the device reservation to another
                               path.

  DISPLAY_BATCH_STATUS      =  To display the status of the batch process.

  COMPARE_FILE              =  To compare two files against each other.

  COPY_FILE                 =  To copy a file to another file or directory.

  LOCATE_FILE               =  To locate the directory the file is in.

  RENAME                    =  To change the name of a file.

  MOVE_FILE                 =  To move a file to another directory.

  DELETE_FILE               =  To delete a file.

  SET_EXPIRATION_DATE       =  To set a date on the file so it won't allow
                               anybody to erase it before that date.

  CREATE_FILE               =  To create and name a new file.

  CREATE_INDEX              =  To create a new index for a file.

  CREATE_DELETED_RECORD_INDEX =  To create a list of reusable locations in a
                                 file.

  CREATE_RECORD_INDEX       =  To create an index used to map records into
                               a file and re-use space made available by
                               deletions.
                               (Once created, it is updated forever.)

  DELETE_INDEX              =  To delete a set of indexes to a file.

  DISPLAY_FILE_STATUS       =  To display information about a set of files
                               that you specify.

  DUMP_FILE                 =  To dump the contents of a file in HEX and
                               ASCII onto the screen for debugging.

  DUMP_RECORDS              =  To dump one or more records in a fixed,
                               sequential, relative, or stream file.

  ENFORCE_REGION_LOCKING    =  To turn mandatory region locking on/off for
                               one or more stream files.

  SET_FILE_ALLOCATION       =  To set the number of additional disk blocks
                               that the operating system allocates for a
                               file each time the file needs more disk
                               space.

  SET_IMPLICIT_LOCKING      =  To turn implicit locking on/off for a file or
                               files.  When it is on, the system overrides
                               an attempt to open the file with a
                               different locking specification.

(*****************************************************************************)

$Note$
```

If you need any more help with the commands please try their on-line help program by typing HELP when you are logged in or HELP <Command> and please excuse the format of the command listings but if you would like a better listing look for the COMPLETE informational guide to VOS systems by Dr. No-Good.

(**********)

Security

The basic security for VOS uses ACL or ACCESS_CONTROL_LISTS. These are lists that the creator of a directory or file make by using the GIVE_ACCESS command. There are four kinds of security you can have. They are as follows:

For file security:

NULL	-+-	That means you can't do anything with it.
READ	-+-	You can READ it but not modify it.
WRITE	-+-	That means you have READ and WRITE access to it so you can modify it.
EXECUTE	-+-	That means they can read it and run it.

For directory security:

MODIFY	-+-	That means you can add, remove, change, and execute files in the directory.
STATUS	-+-	That means you can display_dir_status and view the current status of the directory.
NULL	-+-	That means you can not access the directory.

If you don't have the appropriate security for the directory or file it is because the owner/creator of the file or directory doesn't have you on the list and since this informational file doesn't contain the information needed to get access to files that you haven't been given access to then it is advisable to look for more informational files from [ECHO].

Volume Four, Issue Thirty-Seven, File 9 of 14

THE COMPUSERVE CASE
A STEP FORWARD IN FIRST AMENDMENT PROTECTION FOR ONLINE SERVICES

Presented by Electronic Frontier Foundation

Introduction

by Mike Godwin (mnemonic@eff.org) in EFFector Online 3.03

By now you may have heard about the summary-judgment decision in Cubby, Inc. v. CompuServe, a libel case. What you may not know is why the decision is such an important one. By holding that CompuServe should not be liable for defamation posted by a third-party user, the court in this case correctly analyzed the First Amendment needs of most online services. And because it's the first decision to deal directly with these issues, this case may turn out to be a model for future decisionsin other courts.

The full name of the case, which was decided in the Southern District of New York, is Cubby Inc. v. CompuServe. Basically, CompuServe contracted with a third party for that user to conduct a special-interest forum on CompuServe. The plaintiff claimed that defamatory material about its business was posted a user in that forum, and sued both the forum host and CompuServe. CompuServe moved for, and received, summary judgment in its favor.

Judge Leisure held in his opinion that CompuServe is less like a publisher than like a book store owner or book distributor. First Amendment law allows publishers to be liable for defamation, but not bookstore owners, because holding the latter liable would create a burden on bookstore owners to review every book they carry for defamatory material. This burden would "chill" the distribution of books (not to mention causing some people to get out of the bookstore business) and thus would come into serious conflict with the First Amendment.

So, although we often talk about BBSs as having the rights of publishers and publications, this case hits on an important distinction. How are publishers different from bookstore owners? Because we expect a publisher (or its agents) to review everything prior to publication. But we *don't* expect bookstore owners to review everything prior to sale. Similarly, in the CompuServe case, as in any case involving an online service in which users freely post messages for the public (this excludes Prodigy), we wouldn't expect the online-communications service provider to read everything posted *before* allowing it to appear.

It is worth noting that the Supreme Court case on which Judge Leisure relies is Smith v. California -- an obscenity case, not a defamation case. Smith is the Supreme Court case in which the notion first appears that it is generally unconstitutional to hold bookstore owners liable for content. So, if Smith v. California applies in a online-service or BBS defamation case, it certainly ought to apply in an obscenity case as well.

Thus, Cubby, Inc. v. CompuServe sheds light not only on defamation law as applied in this new medium but on obscenity law as well. This decision should do much to clarify to concerned sysops what their obligations and liabilities are under the law.

- -

Highlights of the CompuServe Decision

by Danny Weitzner (djw@eff.org) in EFFector Online 3.03

"CompuServe's CIS [CS Information Service] product is in essence an electronic, for-profit library that carries a vast number of publications and collects usage and membership fees from its subscribers in return for access to the

publications. CompuServe and companies like it are at the forefront of the information industry revolution. High technology has markedly increased the speed with which information is gathered and processed; it is now possible for an individual with a personal computer, modem, and telephone line to have instantaneous access to thousands of news publications from across the United States and around the world. While CompuServe may decline to carry a given publication altogether, in reality, once it does decide to carry a given publication, it will have little or no editorial control over that publication's contents. This is especially so when CompuServe carries the publication as part of a forum that is managed by a company unrelated to CompuServe. "... CompuServe has no more editorial control over ... [the publication in question] ... than does a public library, book store, or newsstand, and it would be no more feasible for CompuServe to examine every publication it carries for potentially defamatory statements than it would for any other distributor to do so."

"...Given the relevant First Amendment considerations, the appropriate standard of liability to be applied to CompuServe is whether it knew or had reason to know of the allegedly defamatory Rumorville statements."

Cubby, Inc. v. CompuServe, Inc. (90 Civ. 6571, SDNY)

- -

For the full opinion, please see:

CUBBY, INC., a Corporation d/b/a SKUTTLEBUT, and ROBERT G. BLANCHARD, Plaintiffs, v. COMPUSERVE INC., d/b/a RUMORVILLE, and DON FITZPATRICK, individually, Defendants

No. 90 Civ. 6571 (PKL)

UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK

October 29, 1991, Decided
October 29, 1991, Filed

```
PWN ^*^ PWN ^*^ PWN { WeenieFest'92 } PWN ^*^ PWN ^*^ PWN
^*^                                                 ^*^
PWN         P h r a c k   W o r l d   N e w s       PWN
^*^         ~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~~       ^*^
PWN            Special Edition Issue Five           PWN
^*^                                                 ^*^
PWN                  "WeenieFest '92"               PWN
^*^                                                 ^*^
PWN           ~A Meeting With John Markoff~         PWN
^*^                                                 ^*^
PWN               Written by Count Zero             PWN
^*^                                                 ^*^
PWN ^*^ PWN ^*^ PWN { WeenieFest'92 } PWN ^*^ PWN ^*^ PWN
```

WeenieFest '92: A Meeting With John Markoff
Co-Author of CYBERPUNK: Outlaws and Hackers on the Computer Frontier

..oooOO Count Zero OOooo..

count0@world.std.com

- -

"Boston Computer Society General Meeting, Wednesday, January 22, 7:30pm. Katie Hafner, co-author with husband John Markoff of _Cyberpunk_, talks about computer ethics [ya, right] and computer crimes. _Cyberpunk_ details the stories of three computer hackers: Kevin Mitnick, an expert phone phreak, who carried his hacking to obsession [isn't that a perfume?] and addiction-wreaking havoc [holy SHIT!] with computer networks and top-secret research; Pengo, from Germany, who penetrated US military computers and sold information to the Soviet Union; and Robert Morris, a Harvard and Cornell graduate, who released a virus [WORM!] program that crippled thousands of computers on Internet. This discussion may change how you think about computer accessibility [sure changed MY life..jeesh]."

That's how the advertisement appeared in the Boston Computer Society's UPDATE mag (without my bracketed snide comments, of course). Knight Lightning informed me of this meeting via electronic mail, and I read it the DAY it was happening. I had read about half of the book CYBERPUNK, and I know most of you have already checked it out. Yes, it is a piece of shit. A great deal of the info is *fabricated*, and the authors attempt to explain hacking as a "social disorder"...on par with juvenile delinquency.

True, a lot of hacking is just kids screwing around, but there is MORE to the scene than just that. What about the violation of civil liberties going on by the federal government and its agents? What about privacy on the nets? What about the REAL DRIVE behind most of the hacking going on today... the search for TECH KNOWLEDGE? These topics were NOT covered adequately in the book.

Seeing this meeting as a GREAT opportunity to grill Ms. Hafner and to hear what members of the BCS had to say, I attempted to quickly mobilize the entire RDT crew into attending. Alas, I was the *only* person able to make it. "What the hell," I figured, "I'm sure there'll be plenty of other people there who'll make the discussion lively and *heated*." Boy, was I wrong...

For starters, Ms. Hafner was unable to attend. Instead, her husband and co-author, John Markoff showed up. I had never been to a BCS meeting before, and figured that the members would be relatively intelligent about computers and computer ethics. Well, about 80 people filled the lecture hall, and ALL of them were older than me (and I'm 24 by the way). Looked like mostly yuppie trash ("Gee, I just bought this 486...I wonder what it does. Guess I'll join the BCS!") and some old professor-types. Suddenly, I felt a chill... *Weenie-alert* Two bozos behind me were trying to discuss how to write an MS-DOS CONFIG.SYS file:

"Bob, my computer is all messed up. Doesn't work."
"Gee, well, maybe you need one of those set device equals things!"

NOTE: ALL quotes are REAL...Yes, truth is stranger than fiction...

Oh well...Finally, John Markoff came on-stage looking a lot like Dustin Hoffman. He started out by talking for 15 minutes on the definitions of "hacker," "cracker," and "cyberpunk." This is when my migraine started (a small throbbing pulse in my left temple). He discussed the origin of the term "cyberpunk" and made MANY references to *BILL* Gibson. Guess he wanted to stroke himself and make his "personal" relationship with Gibson known to all. Then, he talked in DETAIL about how HE figured out who set loose the Internet worm. "I told them to 'finger RTM'... and the name Robert T. Morris popped up." Boy, some SERIOUS tech wizardry going on there. Markoff patted himself on the back for about 10 minutes more. He also seemed proud of his dealings with Cliff Stoll (as he plugged THE CUCKOO'S EGG about 5 times). Stroke, stroke, stroke. He seemed really *proud* at having discovered all this info about the computer underground (even though his book is ONLY about *THREE* case studies!!!).

"We wanted to get inside these cultures..."

Well his book was basically just a REPORT of WHAT HAPPENED (not even factual half the time)... NOT about the CULTURE... NOT about what really made these people tick... NOT about what REALLY ATTRACTS people to the computer underground. He was just a *reporter*, looking for a scoop. Nothing more.

After describing his book, he opened up the presentation to discussion. The FIRST question was by some BCS dork:

"Do you know anything about the printer-ROM virus used in the Iraqi computer systems?"

I got a sick feeling in my stomach. Markoff talked about this for 10 minutes with comments by other BCS members thrown in. ARRRGH. Anyway, the NEXT question was a real winner:

"What about those computers that took the Turing test recently.. did they pass? Could you explain what a Turing test is?"

So maybe the BCS people WERE NOT that up on things. Maybe none of them read the book. Maybe none of them have ever read Phrack or 2600. Maybe ALL of them have their heads shoved up their butts?

Finally, I made my move. I asked him:

"What do you think of the punishments given to convicted 'cyberpunks'? Do you think they're fair? What about seizure of equipment without charges, taking examples from Operation Sundevil?"

Markoff: "I think the government is just using scare tactics. It's a shame that equipment is seized. It's unconstitutional."

Yep, that is all he had to say about it. No comments on the POLICE STATE that's evolving on the nets. Nothing about what's being done to *protect* computer users' free speech. Next question of mine:

"What do you think really drives 'cyberpunks'...how 'serious' do you think the *crime* of *hacking* is?"

Markoff: "It's just juvenile delinquency. Most of it has nothing to do with tech wizardry. It's mostly con-artists. I hope there is a 'fad element' to this cyberpunk thing. Hopefully they'll grow out of it."

Yeah, this guy certainly has his damn FINGER on the PULSE of the underground. We're just a bunch of delinquent, juvenile con-artists. We'll grow out of it. Really. Man, I was steamed. What he said was full of *half-truths* leaving out IMPORTANT things, like the drive for exploration of highly complicated networks and machinery, but I wasn't going to pick a fight

with this guy. I calmed down and asked the next question on my list:

"What do you think of publications like Phrack and 2600? How do you feel about the E911 bust that tried to suppress Phrack?"

Markoff: "I don't buy their 'exploration' excuse. I don't want people testing the locks on MY computer. It's just juvenile delinquency."

How insightful. Completely ignored my question about the E911 affair. So much for understanding the underground. Ya, we all read stuff like Phrack and 2600 JUST so we can FUCK UP things.

***ONE interesting thing he mentioned was that MOST hacker-related crimes are INSIDE JOBS. Trusted people working on the INSIDE. Well, that was the ONLY thing he said that I totally agreed with. At least Markoff isn't trying to start a "Cyberpunk Witch-Hunt"...not like OTHER people (i.e., Geraldo, Don Ingram, etc.).

This gets REAL funny now. Other BCS members seemed to have NO interest in talking about hacking/phreaking/civil liberties/hacker ethic/etc. ONE guy asked:

"Is piracy a big problem in the US?"

Another asked:

"Do pirate bulletin boards still exist?"

Some *insightful* BCS member said:

"Yeah, but it's dangerous. Lawyers call up and check to see if you have copyrighted software. You can go to jail for it!"

Markoff: "Yes, piracy is still rampant. I can't give you any numbers <cheesy smile here> but I know many exist."

BCS member responds:

"You mean I can just call a number and get Pagemaker for free?"

At this point, I vomited violently..at least my BRAIN did. Many other stupid questions were asked, but I won't torture you further ("What about the IBM/Apple merger?"...that sort of thing). I managed to get in ONE LAST question:

"What do you think of 'reformed cyberpunks'...for nstance, the security consulting company 'Comsec' formed by ex-LOD members?"

Markoff: "I think that any company that hires them should know what they're getting into. I'm skeptical. *I* wouldn't hire them."

You should know that at this point MOST of the BCS dorks laughed out loud, in annoying, weenie-like chuckles of mirth. It took all of my strength not to get up and crack skulls. So much for intelligent discussions. Actually, throughout MOST of the meeting, people were laughing for no apparent reason. Guess they knew something I didn't?

In the final analysis, the meeting confirmed my suspicions that Markoff is just a reporter trying to make a buck. Cashing in on half-truths. Not at all interested in the "cyberpunk's" point of view. Not interested in the ETHICS and MORAL RAMIFICATIONS of hacker busts. He's just reporting the "news." At least he wasn't trying to stir up a "witch-hunt"...but then again, he isn't contributing much to the awareness of the underground and what it "really" means...hacking is NOT a sickness...it is NOT something to "grow out of"... it means freedom of speech...freedom to explore (to an extent..heh) and the DESIRE to explore. MUCH more than juvenile delinquency. I hope someone writes a book from that perspective someday.

I also got an insight into the BCS community. Clueless. Need I say more?

I hope you enjoyed this file. Look for more "Special Reports" in the near future.

```
:   -=Restricted -=Data -=Transmissions    :
:                                          :
: "Truth is cheap, but information costs." :
```

PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN PWN
PWN Phrack World News PWN
PWN PWN
PWN Issue XXXVII / Part One of Four PWN
PWN PWN
PWN Compiled by Dispater & Spirit Walker PWN
PWN PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN

Federal Seizure Of "Hacker" Equipment — December 16, 1991

By Barbara E. McMullen & John F. McMullen (Newsbytes)

"New York's MOD Hackers Get Raided!"

NEW YORK CITY -- Newsbytes has learned that a joint Unites States Secret Service / Federal Bureau of Investigation (FBI) team has executed search warrants at the homes of so-called "hackers" at various locations across the country and seized computer equipment.

It is Newsbytes information that warrants were executed on Friday, December 6th in various places including New York City, Pennsylvania, and the state of Washington. According to informed sources, the warrants were executed pursuant to investigations of violations of Title 18 of the federal statutes, sections 1029 (Access Device Fraud), 1030 (Computer Fraud and Abuse Act), 1343 (Wire Fraud), and 2511 (Wiretapping).

Law enforcement officials contacted by Newsbytes, while acknowledging the warrant execution, refused to comment on what was called "an on-going investigation." One source told Newsbytes that the affidavits underlying the search warrants have been sealed due to the on-going nature of the investigation."

He added "There was obviously enough in the affidavits to convince judges that there was probable cause that evidence of a crime would be found if the search warrants were issued."

The source also said that he would expect a statement to be issued by the Secret Service/FBI team "somewhere after the first of the year."

Two Cornell Students Arrested for Spreading Computer Virus — February 27, 1992

By Lee A Daniels (New York Times News Service)
Special Thanks: Risks Digest

Two Cornell University undergraduates were arrested Monday night and charged with developing and spreading a computer virus that disrupted computers as far away as California and Japan, Cornell officials said. M. Stewart Lynn, vice president for information technologies at the university in Ithaca, N.Y., identified the students as David Blumenthal and Mark Pilgrim. Lynn said that both Blumenthal, who is in the engineering program, and Pilgrim, in the college of arts and sciences, were 19-year-old sophomores. They were arrested on the evening of February 24 by Cornell and Ithaca police officers. Lynn said the students were arraigned in Ithaca City Court on charges of second-degree computer tampering, a misdemeanor, and taken to the county jail. Lynn said authorities believed that the two were responsible for a computer virus planted in three Macintosh games on February 14.

He identified the games as Obnoxious Tetris, Tetricycle and Ten Tile Puzzle. The virus may have first appeared in a Stanford University public computer archive and spread from there through computer users who loaded the games into their own computers.

Lynn said officials at Cornell and elsewhere became aware of the virus last week and quickly developed what he described as "disinfectant" software to

eradicate it. He said officials traced the virus to Cornell last week, but he would not specify how that was done or what led officials to the two students. Lynn said he did not yet know how much damage the virus had caused. "At Cornell we absolutely deplore this kind of behavior," he said.

Note: References to the Robert Morris, Jr. virus incident at Cornell deleted. Associated Press reported that both defendants are being held in the Tompkins County Jail on $10,000 bail.

Man Admits to NASA Hacking November 26, 1991

By John C Ensslin (Rocky Mountain News)(Page 6)
Also see Phrack 34, File 11
Special Thanks: The Public

A self-taught computer hacker with a high school education admitted Monday to breaking into a sensitive NASA computer system -- in less time than it takes the Broncos to play a football game.

Richard G. Wittman Jr., 24, told Denver U.S. District Judge Sherman Finesilver that it took him about "1 1/2 to 2 hours" on a personal computer using telephone lines in his apartment to tap into the space agency's restricted files.

Wittman pleaded guilty Monday to one felony count of altering information -- a password -- inside a federal computer. In exchange for the plea, federal prosecutors dropped six similar counts in indictments handed up in September.

The Northglenn High School graduate told the judge he hadn't had much schooling in computers. Most of what he knew about computers he learned from books. And most of those books, he said, are in a federal warehouse, seized after FBI agents searched his Westminster apartment last year.

"Do you think you could teach these two lawyers about computers?" Finesilver asked, referring to Wittman's public defender and the prosecutor. "Probably," Wittman replied.

Wittman not only broke into 118 NASA systems, he also reviewed files and electronic mail of other users, said assistant U.S. attorney Gregory C. Graf.

It took NASA investigators nearly 300 hours to track Wittman an another 100 hours to rewrite the software, Graf said.

Wittman faces up to five years in prison and a $250,000 fine. But Graf said the government will seek a much lighter penalty when Wittman is sentenced in Jan. 13.

Both sides have agreed on repayment of $1,100 in collect calls placed to the other computer system. But they differ on whether Wittman should be held responsible for the cost of new software.

Hacker Pleads Guilty December 5, 1991

Special Thanks: Iron Eagle

"A 24-year-old Denver hacker who admitted breaking into a sensitive NASA computer system pleaded guilty to a felony count of altering information.

In exchange for the plea Monday, federal prosecutors dropped six similar counts against Richard G. Wittman Jr., who faced up to five years in prison and a $250,000 fine. Authorities said the government will seek a much lighter penalty when Wittman is sentenced January 13.

Both sides have agreed on repayment of $1,100 in collect calls he placed to the computer system, but they differ on whether Wittman should be held responsible for the cost of new software.

Wittman told U.S. District Judge Sherman Finesilver that it took him about two hours on a personal computer in his apartment to tap into the space agency's restricted files. It took NASA investigators nearly 300 hours to track Wittman and an additional 100 hours to rewrite the software to prevent a recurrence, prosecutors said."

Recent Novell Software Contains A Hidden Virus December 20, 1991

By John Markoff (New York Times)

The nation's largest supplier of office-network software for personal computers has sent a letter to approximately 3,800 customers warning that it inadvertently allowed a software virus to invade copies of a disk shipped earlier this month.

The letter, sent on Wednesday to customers of Novell Inc., a Provo, Utah, software publisher, said the diskette, which was mailed on December 11, had been accidentally infected with a virus known by computer experts as "Stoned 111."

A company official said yesterday that Novell had received a number of reports >from customers that the virus had invaded their systems, although there had been no reports of damage.

But a California-based computer virus expert said that the potential for damage was significant and that the virus on the Novell diskette frequently disabled computers that it infected.

MASSIVE POTENTIAL LIABILITIES

"If this was to get into an organization and spread to 1,500 to 2,000 machines, you are looking at millions of dollars of cleanup costs," said John McAfee, president of McAfee & Associates, a Santa Clara, Calif. antivirus consulting firm. "It doesn't matter that only a few are infected," he said. "You can't tell. You have to take the network down and there are massive potential liabilities." Mr. McAfee said he had received several dozen calls from Novell users, some of whom were outraged.

The Novell incident is the second such case this month. On December 6, Konami Inc., a software game manufacturer based in Buffalo Grove, 111.wrote customers that disks of its Spacewrecked game had also become infected with an earlier version of the Stoned virus. The company said in the letter that it had identified the virus before a large volume of disks had been shipped to dealers.

SOURCE OF VIRUS UNKNOWN

Novell officials said that after the company began getting calls earlier this week, they traced the source of the infection to a particular part of their manufacturing process. But the officials said they had not been able to determine how the virus had infected their software initially.

Novell's customers include some of nation's largest corporations. The software, called Netware, controls office networks ranging from just two or three machines to a thousand systems.

"Viruses are a challenge for the marketplace," said John Edwards, director of marketing for Netware systems at Novell. "But we'll keep up our vigilance. He said the virus had attacked a disk that contained a help encyclopedia that the company had distributed to its customers.

SERVERS SAID TO BE UNAFFECTED

Computer viruses are small programs that are passed from computer to computer by secretly attaching themselves to data files that are then copied either by diskette or via a computer network. The programs can be written to perform

malicious tasks after infecting a new computer, or do no more than copy themselves from machine to machine.

In its letter to customers the company said that the Stoned 111 virus would not spread over computer networks to infect the file servers that are the foundation of networks. File servers are special computers with large disks that store and distribute data to a network of desktop computers.

The Stoned 111 virus works by attaching itself to a special area on a floppy diskette and then copying itself into the computer's memory to infect other diskettes.

But Mr. McAfee said the program also copied itself to the hard disk of a computer where it could occasionally disable a system. In this case it is possible to lose data if the virus writes information over the area where a special directory is stored.

Mr. McAfee said that the Stoned 111 virus had first been reported in Europe just three months ago. The new virus is representative of a class of programs known as "stealth" viruses, because they mask their location and are difficult to identify. Mr. McAfee speculated that this was why the program had escaped detection by the company.

STEPS TOWARD DETECTION

Novell has been moving toward adding new technology to its software to make it more difficult for viruses to invade it, Mr. Edwards said. Recently, the company licensed special digital-signature software that makes it difficult for viruses to spread undetected. Novell plans to add this new technology to the next major release of its software, due out at the end of 1992.

In the past, courts have generally not held companies liable for damages in cases where a third party is responsible, said Susan Nycum, a Palo Alto, California, lawyer who is an expert on computer issues. "If they have been prudent it wouldn't be fair to hold them liable," she said. "But ultimately it may be a question for a jury."

Working Assets Long Distance! January 1992
~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Taken from an advertisement in Mother Jones

(Not pictured is a photo of a college student giving "the finger" to someone and a caption that reads 'Twenty years later, we've given people a better way to put this finger to use.')

The advertisement reads as follows:

- -

Sit-ins. Protest marches, Flower power. Times have changed but the need for grass roots involvement hasn't.

Introducing "Working Assets Long Distance." The ONLY phone company that is as committed to social and political change as you are. Every time you use your finger to make a long distance call, one percent of the bill goes to non-profit action groups at no cost to you. Hard-hitting advocacy groups like AMNESTY INTERNATIONAL, GREENPEACE, PLANNED PARENTHOOD, FEDERATION OF AMERICA, THE AMERICAN CIVIL LIBERTIES UNION, and many others.

We're more than a phone company that gives money to good causes. Our intent is to make your individual voice heard. That's why we offer *FREE CALLS* to corporate and political leaders. And well-argued letters at a fraction of the cost of a mail-gram. So you can demand a halt to clear-cutting our ancient forests or let Senators know how you feel about important issues like reproductive rights. It's that simple. Your phone becomes a tool for democracy and you don't give up a thing. You see, Working Assets comes with the exact same service as the major long distance carriers. Convenient
~~~~~~~~~~~~~~~~~~~~~~~~~~~~

dial 1 calling 24-hour operation and fiber optic sound quality. All this at rates lower that AT&T's basic rates. And signing up couldn't be simpler.

Just give us a call at 1-800-788-8588 ext 114 or fill out the coupon today. We'll hook you up right away without any intrusion or interruption. So you can help change the world without lifting a finger. Ok, maybe one finger.

Computer Virus Used in Gulf War January 12, 1991
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Taken from The Boston Globe (Page 12)
Special Thanks: Tone Surfer

Several weeks before the start of the Gulf War, US intelligence agents inserted a computer virus into a network of Iraqi computers tied to that country's air defense system, a news magazine reports. US News and World Report said the virus was designed by the supersecret National Security Agency at Fort Meade, Maryland, and was intended to disable a mainframe computer.

The report, citing two unidentified senior US officials, said the virus appeared to have worked, but it gave no details. It said the operation may have been irrelevant, though, since the allies' overwhelming air superiority would have ensured the same results of rendering the air defense radars and missiles ineffective. The secret operation began when American intelligence agents identified a French made computer printer that was to be smuggled from Amman, Jordan, to a military facility in Baghdad.

The agents in Amman replaced a computer chip in the printer with another micro-chip that contained the virus in its electronic circuits. By attacking the Iraqi computer through the printer, the virus was able to avoid detection by normal electronic security procedures, the report said. "Once the virus was in the system, the US officials explained, each time an Iraqi technician opened a "window" on his computer screen to access information, the contents of the screen simply vanished," US News reported.

The report is part of a book, based on 12 months of research by US News reporters, called "Triumph without Victory: The Unreported History of the Persian Gulf War," to be published next month.

Indictments of "Information Brokers" January 1992
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Taken from The Privacy Journal

The unholy alliance between "information brokers" and government bureaucrats who provide personal information has been uncovered in the grand jury indictments of 18 persons in 14 states.

United States Attorney Michael Chertoff in Newark, New Jersey, and his counterpart in Tampa, Florida, accused eight "information brokers" (or "information gatekeepers" or "super bureaus") of bribing two Social Security Administration employees to provide confidential earnings and employee information stored in federal computer files. The brokers, who fill in the cracks not occupied by national credit bureaus and who also track the whereabouts of persons, would sell the information to their clients -- retailers, lawyers, detectives, insurance companies, and others.

Ned Flemming, president of Super Bureau Inc. of Montery, California, was indicted on 32 counts for coaxing a Social Security supervisor in New Jersey named Joseph Lynch (who was not charged) to provide confidential personal information for a fee. Fleming's daughter, Susan, was charged also, as were Victor Fought, operator of Locate Unlimited in Mesa, Arizona; George T. Theodore, owner of Tracers Worldwide Services in Corpus Christi, Texas; Richard Stone, owner of Interstate Information Services in Port Jefferson, New York; and Michael Hawes, former owner of International Criminal Investigative Agency (ICIA) in Port Angeles, Washington, for participating in the same conspiracy. Another broker, Joseph Norman Dillon Ross, who operates a firm under his name in Pauma Valley, California also accepted the personal data,

according to Chertoff, but was not charged. Richard Stone was further indicted for corrupting a Social Security claims clerk in Melrose Park, Illinois. Also charged were Allen Schweitzer and his wife Petra, who operate Security Group Group in Sumner, Washington.

The government employees also stole personal information from the FBI's National Crime Information Center (NCIC), which stores data on arrests and missing persons.

Fleming told Privacy Journal that he had never met Lynch. Stone refused to comment. Tracers Worldwide, ICIA, and Locate Unlimited are not listed in telephone information, although all three companies are required by the Fair Credit Reporting Act to permit the subjects of their files to have disclosure of such information to them.

The 18-month long investigation culminating in the December 18 indictments and arrests is only the first phase, said Assistant U.S. Attorney Jose Sierra. "We don't think it stops there."

For the past three years, the Big Three credit bureaus have continued to sell credit information regularly to information brokers, even after complaints that some of them violated the Fair Credit Reporting Act in disclosing credit information for impermissible purposes. Trans Union's president, Albert Flitcraft, told Congress in 1989 that is was not possible for a major credit bureau to protect consumer information sold to brokers. John Baker, Equifax senior vice-president, said at the time that the Big Three would "put together our best thinking" to see if safeguards could be developed. By 1991, Oscar Marquis, vice-president of Trans Union, was asking Congress for solutions, but Baker presented Equifax's new guidelines and checklist for doing business with the brokers. None of the Big Three has been willing to cease doing business with the cloudy merchants of recycled credit reports -- and of purloined Social Security and FBI information.

- -

Meanwhile, at the Internal Revenue Service...

Two weeks after he blew the cover off the information brokers, U.S. Attorney Michael Chertoff in New Jersey indicted a retired chief of the Internal Revenue Service Criminal Investigation Division for selling personal information to a California private investigative firm in his last week on the job in 1988.

For a $300 payment, according to the indictment, the IRS executive, Robert G. Roche, promised to procure non-public marital records from vital records offices. Using false pretenses, he ordered one of his subordinates to get the information, on government time. The aide got the records in one instance only after writing out an IRS summons and in another instance after producing a letter on IRS stationary saying the information was needed for "official investigative matters." Roche, according to the U.S. Attorney, accepted payment from the California investigative firm of Saranow, Wells, & Emirhanian, part of a larger network called Financial Investigative Services Group.

- -

The Privacy Journal is an independent monthly on privacy in the computer age. They can be reached at:

Privacy Journal
P.O Box 28577
Providence, Rhode Island 02908
(401)274-7861

SSA, FBI Database Violations Prompt Security Evaluations January 13, 1992
~~~~~~

By Kevin M. Baerson (Federal Computer Week)(Pages 1, 41)

Indictments recently handed down against insiders who bought and sold
~~~~~~

confidential information held in Federal Bureau of Investigation and Social Security Administration computers have prompted agency officials to evaluate how well the government secures its databases.

"I see this as positive more than negative," said David Nemecek, section chief for the FBI's National Crime Information Center (NCIC), which contains data on thousands of people suspected and convicted of crimes. "Am I happy it happened? No. But it led us to discovering that this was happening and it sends a message that if people try it, they will get caught."

But Renny DiPentima, assistant commissioner of SSA's Office of System Design and Development, said he did not view the indictments as a positive development.

"It's not a victory," DiPentima said. "Even if we catch them, it's a loss. My victory is when I never have a call that someone has abused their position."

The "information broker" bust was the culmination of an 18-month investigation by the Department of Health and Human Services' inspector general's office in Atlanta. Officials said it was the largest case ever prosecuted involving the theft of federal computer data. More indictments could be forthcoming, they said.

Special agents from the FBI joined the inquiry and in the end nabbed 18 people >from 10 states, including one former and two current SSA employees. Others indicted were a Chicago police officer, an employee of the Fulton County Sheriff's Office in Georgia, and several private investigators.

The indictments alleged that the investigators paid for confidential data, including criminal records and earnings histories, that was lifted from the databases by people who exploited their access to the records.

"The FBI cannot manage every person in the United States," Nemecek said. "We have all kinds of protection to prevent this from happening. We keep logs of who uses the systems and for what, security training programs and routine audits of inquiries."

"But the people who committed the violations had access to the system, and there's only one way to deal with that: aggressive prosecution of people who do this. And the FBI is actively pursuing these individuals."

DiPentima's problem is equally delicate. His agency performs 15 million electronic transactions per day -- 500 per second -- and monitoring the rights and wrongs of those people is a daunting task.

Currently, every employee who uses the network is assigned a password and personal identification number, which change frequently. Depending on the nature of the employee's job, the PIN grants him access to certain types of information.

If the employee tries to access a menu in the system that he has not been authorized to enter, or makes more than one error in entering his PIN number, he is locked off the system. Once that happens, only a security office from one of SSA's 10 regional offices can reinstate the employee.

An SSA section chief and six analysts, working from the agency's data center headquarters outside Baltimore, also search routinely for transactional aberrations such as employees who have made an unusual number of transactions on a certain account.

The FBI also has a number of security precautions in place. FBI personnel conduct random audits of searches, and Nemecek said sweeping state and local audits of the system are performed biannually. Furthermore, if the FBI desires, it easily can track an access request back to the terminal and user it came from.

DiPentima said that in the wake of the indictments, he is considering new policies to clamp down on abusers.

Nemecek said that as the FBI continues upgrading the NCIC database, the center might automate further its auditing of state and local agencies to detect patterns and trends of use the way SSA does.

But despite efforts to tighten the screws on network security, both men realize that in cases of federal and municipal employees who exploit authorized access, technology and policies can only go so far in affecting human nature.

Free University Suffers Damage. February 24, 1992

By The Dude (of Holland)

An investigation by the Amsterdam police, in cooperation with an anti-fraud team of the CRI (sort of like the FBI), and the geographical science department of the Free University has led to the arrests of two hackers. The two had succeeded to break into the department's computer system and caused damage of over 100,000 Dutch Guilders.

In a press conference, held by the research teams last Friday, it was stated that the duo, a 25-year old computer-science engineer R.J.N. from Nuenen [aka Fidelio] and a 21-year old student computer-science H.H.H.W. from Roermond [aka Wave], were the first "hackers" to be arrested in the Netherlands. In several other countries this has already happened before.

The arrested hackers made a complete confession. Since November 1991, they have entered the University's computer between 30 and 40 times. The system was known as "bronto." From this system the hackers were able to gain access to other systems, thus travelling to systems in the US, Scandinavia, Spain and Italy.

According to the leader of the computer-crime team of the Amsterdam police, D. Komen, the two cracked codes of the VU-system to get in. They got their hands on so-called "passwords" of officially registered users, which allowed them to use the system at no cost. They were also able to get the "highest of rights" within the computer system "bronto."

A total of four houses were searched, and several PC's, printouts and a large quantity of diskettes was seized. The duo was taken to the DA and imprisoned. Because "hacking" is not a criminal offense in the Netherlands, the suspects are officially accused of falsification of records, destruction of property, and fraud.

This year the government expects to enact legislation that will make hacking a criminal offense, according to P.Slort of the CRI.

The hacker-duo stated that they undertook their illegal activities because of fanatic "hobbyism." "It's a kick to see how far you can go", says Mr. Slort of the CRI. The two said they did not know that their data journeys had caused enormous damages. The police do not see them as real criminals, either since the pair did not earn money from their activities.

Computer Engineer Gets Death Sentence February 9, 1992

Special Thanks: Ninja Master

Richard Farley was cool to the end, taking a sip of water and smoothing his jacket before leaving the courtroom where he was sentenced to die for killing seven people in a rage over unrequited love.

"I'm not somebody who is demonstrative or prone to shedding tears", Farley said Friday before apologizing for the slayings. "I do feel sorry for the victims....I'm not a perfect human being. I'm good. I'm evil."

Farley was convicted in October of the 1988 slayings at ESL Inc., a Sunnyvale defense contractor. Jurrors on November 1st recommended the death penalty for

the computer engineer, who prosecutors said planned the rampage to get the attention of a former co-worker who rejected him.

Superior Court Judge Joseph Biafore Jr. called Farley a vicious killer who had "complete disregard for human life."

"The defendant...killed with the attention to prove to the object of his unrequited love that he wasn't a wimp anymore," Biafore said.

During the trial, prosecutors detailed Farley's 3 1/2-year obsessive pursuit of Laura Black. He sent her more than 100 letters, followed her day and night, left gifts on her desk, and rifled through confidential personnel files to glean tidbits about her life.

Despite her repeated rejections, Farley persisted and was fired in 1987 for harassing her. A year later, he returned to ESL.

Black, 30, was shot in the shoulder during the rampage, but survived to testify against Farley. She said that about a week before the slayings, she had received a court order to keep him away.

Farley, 43, admitted the killings but pleaded not guilty, saying he never planned to kill but only wished to get Black's attention or commit suicide in front of her for rejecting him.

Farley's attorney, Gregory Paraskou, argued that Farley's judgement was clouded by his obsession with Black and that he was not violent before the slayings and likely would not kill again.

But Asst. Dist. Atty. Charles Constantinides said Farley spent years preparing for the murder by taking target practice and buying weapons, including the firearms and 98 pounds of ammunition he used at ESL.

The judge rejected the defense's request for a modified sentence of life in prison and a request for a new trial. Under California law, Farley's death sentence will be automatically sent to the state Supreme Court for review.

Among those in the courtroom were family members of some of the victims, including four who addressed the judge.

Volume Four, Issue Thirty-Seven, File 12 of 14

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN              Phrack World News              PWN
PWN                                             PWN
PWN       Issue XXXVII / Part Two of Four       PWN
PWN                                             PWN
PWN     Compiled by Dispater & Spirit Walker    PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Operation Sun-Devil Nabs First Suspect

February 17, 1992

By Michael Alexander (ComputerWorld)(Page 15)

"Defendant Pleads Guilty To Possession Of Access Codes, Faces 10-year Term"

The U.S. Department of Justice said last week that it had successfully completed its first prosecution in the Operation Sun-Devil investigation.

Robert Chandler [a/k/a The Whiz Kid and former bulletin board system operator of the Whiz House in 619 NPA], 21, pleaded guilty in federal court in San Diego to a single felony for possessing 15 or more access codes, which can be used illegally to make toll-free telephone calls, said Scott Charney, who heads the Justice Department's computer crime unit in Washington, D.C. Chandler also admitted to using the access codes, Charney said.

Chandler will be sentenced on May 11. The legal maximum penalty is 10 years' imprisonment, but federal prosecutors will probably recommend probation, assuming the sentencing guidelines and the judge handling the case permit it, Charney said.

Chandler may also be required to make restitution of a still-undetermined amount for telephone calls made with the access code.

On May 7 and 8, 1990, U.S. Secret Service and local law enforcement officials executed more than 20 search warrants [more like 27] in 14 cities in a nationwide crackdown on computer crime code called Operation Sun-Devil. Federal law enforcers said the raid was aimed at rounding up computer-using outlaws who were engaged in telephone and credit-card fraud.

Approximately 42 computers and 23,000 disks were swept up in the dragnet, but until last week there were no indictments or convictions in the investigation.

The Justice Department has been severely criticized by Computer Professionals for Social Responsibility (CPSR), the Electronic Frontier Foundation (EFF), and other advocacy groups for its handling of Operation Sun-Devil cases. CPSR has charged that federal law enforcers trampled on the First and Fourth Amendment rights of those targeted in the raids.

No More Fast Times For Spicoli

By Night Ranger

On November 19, 1991, Spicoli was awaken by Pima County (Arizona) Sheriffs and some other agents in his apartment. They showed him their search warrants, which was obtained under the suspicion of "Computer Fraud and/or Theft" and asked him to step outside. They began dismantling his computer system, which ran his bulletin board called "Fast Times." It was not a hack/phreak bulletin board and contained no information that would normally be construed as such. The main reason he ran the board was because he was writing it himself.

The authorities took many items not related to his computer, including his VCR. He was not charged with any crimes and additionally he was informed that he was "free to go." This incident is very similar to what happened with the

hacker "Mind Rape." Late last year, his home was raided and lots of items were seized, but no charges followed.

Spicoli attempted to hire private legal counsel, but discovered that it was beyond his means financially. Since then, he has chosen to go with the public defender's office.

Weeks later, it was revealed that his case concerned an undisclosed, but presumably large amount of stolen money and he was charged with various felonies. He further learned that the authorities had been monitoring him over a period of at least three months. Anyone who had contact with him between August and November should be careful. His computer is now in the hands of the government.

This is the second major bust in Arizona during the last half of 1991. With people like Gail Thackeray residing there and anti-hacker companies such as Long Distance For Less and U.S. West it is definitely not the place for any kind of hacking.

U2 Shakes Up New England Bell February 24, 1992

By Steve Morse (The Boston Globe)(Page 15)

Irish rockers U2 left local telephone operators hasping for breath. In an unprecedented move designed to thwart scalpers, tickets for U2's March 17 show at Boston Garden went on sale through telephone charge only -- and the result was a long morning for the phone company.

"It was complete gridlock. I don't know how else to describe it. The bombed us right out of the water," said Joanne Waddell, a New England Telephone manager. "We expected a lot of calls ... but this was unbelievable. Our operators were clicking away like crazy out there."

The Garden show sold out in 4 1/2 hours, said Doug Borg of Tea Party Concerts, adding that it took that long because there was a two-ticket limit per person -- another step taken to frustrate scalpers.

"The demand was overwhelming. I heard there were a half-million calls in the first hour," said Larry Moulter, president of Boston Garden. The telephone company said exact figures were not yet available, but Moulter's information is consistent with a recent U2 sale in Atlanta, where more than one million calls, many from eager fans with automatic redial, were logged.

"I don't really have a number. It's safe to say thousands, many thousands," said Peter Cronin, a spokesman for New England Telephone. He admitted there were minor delays in getting a dial tone, but that it was "not a serious situation. If people stayed on the line, they'd get dial tone in a few seconds."

There were 100 lines selling sales for the Garden concert. They checked for duplicate names, credit card numbers and addresses (to help enforce the limit of two per person) and caught 'some' attempts to use a card number more than once.

Federal Agents Raid WCFL; Station Silenced, Forced Off Air January 28, 1992

By Patrick Townson (Telecom Digest)

In an unusual move by the Federal Communications Commission, a far southwest suburban radio station in the Chicago area has been forced off the air by the FCC which alleges illegal activity at the station.

WCFL-FM (104.7), a station licensed in Morris, IL with no connection to the station using the same call letters in Chicago several years ago was silenced by FCC officials who raided the station accompanied by members of the United States Marshall's Office on Friday, January 24.

Prompted by complaints from other broadcasters in the Chicago area, an FCC field inspection team on January 16 found WCFL was beaming its signal at more than twice its authorized power of 11,000 watts, and was using a nondirectional rather than directional antenna as called for in its license to operate.

The effect of the violations was to broacast a more powerful signal toward Chicago and elsewhere, and "to increase the likelyhood of interference with other stations," acccording to Dan Emrick, chief of investigations for the FCC's office in Chicago.

The FCC had cited the station for similar offenses in 1990, and fined the owners $3000. Emrick said there was no record of payment.

Tim Spires is the General Manager of WCFL, and an officer of the parent company 'MM Group' which is based in Ohio. Neither Mr. Spires nor other officials of 'MM Group' would make any response to the FCC action which forced the station off the air at 1:00 PM last Friday.

Emrick said federal officers entered the station shortly before 1:00 PM and served the appropriate legal papers on employees on duty. FCC staffers then siezed the broadcasting studio and transmitting equipment. After giving the obligatory sign off message and station identification over the air, power was killed to the transmitter. Employees were ordered to leave the premises, which was closed with a US Marshall's Seal.

Emrick went on to say the station would not be allowed to return to the air until the station settles its account with the FCC and completes construction of a directional antenna. At that point, the station would be permitted to operate 'in probation' while the Commission did further technical inspections, and the probation status would continue for an unspecified period of time afterward.

A press release was finally issued by the 'MM Group' yesterday which said in part that WCFL " ... went off the air voluntarily in order to install a new antenna; bring their transmitter into compliance with FCC regulations and better serve their listening area."

New Cellular Phones Raise A National Security Debate February 6, 1992

By John Markoff (New York Times)(Page D1)

Advocates of privacy rights are challenging the nation's most clandestine intelligence-gathering agency over how much confidentiality people will have when communicating via the next generation of cellular telephones and wireless computers.

The issue has emerged at meetings this week of an obscure committee of telecommunications experts that is to decide what kinds of protections against eavesdropping should be designed into new models of cellular phones. People concerned with privacy are eager to incorporate more potent scrambling and descrambling codes in equipment to prevent the eavesdropping that is so easy and so common in the current generation of cellular phones.

But privacy advocates contend that the industry committee has already decided not to adopt the maximum level of protection because of pressure from the National Security Agency, whose intelligence gathering includes listening in on phone conversations in foreign countries and intercepting data sent by computers. The privacy-rights faction contends that the security agency opposes codes that are hard to crack because the equipment might be used overseas.

"The NSA is trying to weaken privacy technology," said Marc Rotenberg, Washington director of Computer Professionals for Social Responsibility, a public advocacy group organized by computer scientists and engineers. "At stake is nothing less than the future of our privacy in the communications world."

The standards setting group is made up of cellular telephone equipment manufacturers and service providers.

The National Security Agency is the Defense Department Agency in charge of electronic intelligence gathering around the world for use by many other branches of the government. Officials of the agency, who have been participating in the meetings as observers, said their only interest in the matter was insuring that the government's own secure telephones were compatible with the new cellular phones. They said that agency officials have specifically been told not to participate in the standards-setting effort, and indeed some engineers attending the meetings said they have felt no outside pressure.

But other engineers involved in the standards process said the agency's presence had loomed large in earlier technical meetings during the past two years. "I would talk to people and they would say, 'The NSA wouldn't like this, or wouldn't like that,'" said one committee member, who spoke on the condition that he not be identified.

The Agency's Long Reach

The debate is important, the privacy advocates say, not just for cellular phones but for many other emerging technologies that communicate using radio signals, which are easier to intercept than information sent over conventional telephone lines. These include wireless "personal communicators" that transmit and receive data, and portable "notebook" computers.

But the dispute also illustrates that even as the cold war ebbs, the National Security Agency is still wielding influence over many United States high-technology industries. Indeed, executives from a number of high-technology companies say the agency is hampering their efforts to compete for business overseas by forcing them to make products for foreign markets that are different from products sold domestically.

The agency exercises this power in evaluating some of the applications by companies to export high-technology products. In that role, critics say, the agency has opposed exports of equipment fitted with advanced encryption systems that are increasingly vital to modern business.

Buyers Can Shop Elsewhere

The agency's critics say it is almost impossible to contain the proliferation of encryption technologies and that customers who are deterred from buying it in the United States will simply shop abroad or steal the technology.

"The notion that you can control this technology is comical," said William H. Neukom, vice president for law and corporate affairs at Microsoft Corporation, the big software publisher.

Critics also say that it is ludicrous that encryption systems used in popular software programs receive the type of Government scrutiny that might be expected for weapons. "The notion that our our products should be classified as munitions, and treated that way just doesn't make sense at all," Mr. Neukom said.

Privacy advocates have also challenged the committee's intention not to publish the algorithm on which the encryption technology is based. Traditionally, cryptographers have said that the best way to ensure that encryption techniques work is to publish the formulas so they can be publicly tested.

The committee has said that it will not disclose the formula because it does not want to criminals an opportunity to crack the code. But publishing the formula is only a danger only if the formula is weak, said John Gilmore, a Silicon Valley software designer, and privacy advocate. If the formula is strong, disclosing it publicly and letting anyone try to crack it would simply prove it works.

The code, however, is simple to break, say a number of engineers who have

examined it. Several committee members said they realized that the security agency would never permit the adoption of an unbreakable privacy scheme.

"The cynics in the bar would say that you're never going to get anything by the NSA that they can't crack trivially anyway," said Peter Nurse, chairman of the authentication and privacy subcommittee of the standards committee and an engineer at Hughes Network Systems.

NSA Role Denied

But a number of engineers who worked on the technical standard insist that the agency has had no overt role in setting it. "The standard was based on the technical deliberations of some of the best experts in North America," said John Marinho, chairman of the standards committee and an executive at AT&T. He said the committee relied on the NSA only for guidance on complying with United States regulations.

He also said that the new standard would offer far more privacy protection than is available under the present cellular telephone system. Today, although it is against the law to eavesdrop on a cellular telephone conversation, many individuals modify commercial radio scanners so they can receive the frequencies on which cellular calls are transmitted.

FBI Eavesdropping Challenged February 17, 1992
~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Taken from The Washington Post

WASHINGTON -- Cellular telephones and other state-of-the art telecommunications technology are seriously challenging the FBI's ability to listen to the telephone conversations of criminal suspects, law enforcement officials say. The FBI is seeking $26.6 million next year to update its eavesdropping techniques. Normally tight-lipped FBI officials become even more closed-mouthed when the subject of investigative "sources and methods" comes up. But a review of the bureau's 1993 budget request provides an unusual glimpse into the FBI's research on electronic surveillance and its concerns about new technologies.

"Law enforcement is playing catchup with the telecommunications industry's migration to this technology," said the FBI's budget proposal to Congress. "If electronic surveillance is to remain available as a law enforcement tool, hardware and software supporting it must be developed."

The new technologies include digital signals and cellular telephones. At the same time, there has been an increase in over-the-phone transmission of computer data, which can be encrypted through readily available software programs, say industry experts and government officials.

The FBI's five-year research effort to develop equipment compatible with digital phone systems is expected to cost $82 million, according to administration figures.

The FBI effort is just a part of a wider research program also financed by the Pentagon's secret intelligence budget, said officials who spoke on condition of anonymity.

Electronic surveillance, which includes both telephone wiretaps and microphones hidden in places frequented by criminal suspects, is a key tool for investigating drug traffickers as well as white-collar and organized crime.

Conversations recorded by microphones the FBI placed in the New York City hangouts of the Gambino crime family are the centerpiece of the government's case against reputed mob boss John Gotti, now on trial for ordering the murder of his predecessor, Paul Castellano.

Taps on the phones of defense consultants provided key evidence in the Justice Department's long running investigation of Pentagon procurement fraud, dubbed "Operation Ill Wind." But with the advent of digital phone signals, it is
~~~~~~~~~~~~~~~~~~~~~~~~~~~~

difficult to unscramble a single conversation from the thousands that are transmitted simultaneously with computer generated data and images, industry officials said.

"In the old days all you had to do was take a pair of clip leads and a head set, put it on the right terminal and you could listen to the conversation," said James Sylvester, an official of Bell Atlantic Network Services Inc. But digital signal transmission makes this task much more difficult. Conversations are broken into an incoherent stream of digits and put back together again at the other end of the line.

John D. Podesta, a former counsel to the Senate Judiciary's law and technology subcommittee, said the FBI and other law enforcement agencies are simply victims of a technological revolution. For more than 50 years the basic telephone technology remained the same.

Nynex Will Go On-line With Listings February 20, 1992

By Adam M. Gaffin (adamg@world.std.com)(Middlesex News, Framingham, MA)

You can now let your fingers do the walking electronically through the Yellow Pages.

Nynex yesterday announced an online Yellow Pages available to anyone with a computer and modem, becoming the first regional Bell operating company to offer an electronic Yellow Pages database. The 1984 court order that broke up AT&T had barred such efforts, but that provision was overturned last year.

The service, at least at first, will offer listings only, rather than ads, from close to 300 Nynex directories -- the company serves most of New York and New England, except for Connecticut.

Users will also be able to scan UPI news and financial information, according to Kurt Roessner, president of Nynex Information Technologies, the subsidiary that will run the service. Ultimately, the company hopes to begin offering and displaying Yellow Pages-like ads to users, Roessner said yesterday.

Users will require special software to access the information through the Minitel network, a French system that has so far failed to catch on in the U.S. Nynex will provide the software for free to users of MS-DOS, Macintosh, Apple II and Commodore computers, Roessner said.

Roessner said Nynex eventually hopes to offer the service on other, more popular computer networks. Minitel was chosen because Nynex has offered its Yellow Pages information to French subscribers for almost two years, he said.

Nynex will charge 61 cents a minute -- $36.60 an hour -- the same as French users pay. However, Roessner acknowledged this may be more than Americans are willing to pay and that the company will look at lowering the rate.

CompuServe, the nation's largest consumer-oriented computer network, charges $12.80 an hour -- but drops that to just 50 cents an hour to people who use an AT&T directory of national toll-free numbers.

The Nynex project is the latest in a series of efforts by large companies to sell information to consumers via computer. Some, such as an effort by Knight-Ridder in the mid-1980s, have ended in spectacular failure. Last year, Nynex dropped its own information "gateway" service after losing several million dollars. CompuServe and several other online services, however, reportedly earn sizable profits.

Phone-company information services have been surrounded by controversy. Opponents, who include organizations representing newspaper publishers, say it is unfair to allow a company that provides the means of distribution to also offer services -- a common comparison is to a turnpike authority that also ran a trucking company.

Roessner, however, said he hopes the phone company can cooperate with, rather than fight, other potential "information providers." He said he has already talked with officials at a number of newspapers who seem more willing to work with the phone company on joint projects than their national organizations would let on.

Civil Jury Rules Against AT&T in Patent Violation Case February 9, 1992

By Paul Deckelman (United Press International/UPI)

NEW YORK -- A jury ruled American Telephone & Telegraph Company infringed upon somebody else's patent for telephone switching equipment and awarded the plaintiff $34.6 million, an attorney said.

AT&T contends the suit is without merit and said it will appeal the verdict.

The six-member jury at the federal district court in Midland, Texas, returned its verdict after having heard six days of testimony in the case, brought against the telecommunications giant by Collins Licensing L.P., of Dallas.

The plaintiff's lawyer, Joseph Grear, of the Chicago-based firm of Rolf Stadheim Ltd., held out the possibility that the total award could go substantially higher, due to interest accruing back to 1985. An AT&T spokesman dismissed the possibility.

U.S. District Court Judge Lucius Bunton is considering the jury's recommendation.

Grear claimed AT&T's 5ESS digital central office switching device infringed upon a 1976 federal patent for a "Time Space Time (TST) Switch" awarded to the late Arthur A. Collins.

Collins was the founder of Collins Radio Co., now a division of Rockwell International Inc., of El Segundo, California.

"Arthur Collins was a pioneer in the field of digital telecommunications. The jury's verdict provides recognition of Mr. Collins' substantial research and development investment in, and important technical contributions to, the field of digital telephony," Grear said.

AT&T's Network Systems division came out with the device in the early 1980s, using it for central-office telephone switching equipment used to route calls to the proper exchange and number.

The suit, filed in December 1990, originally named Southwestern Bell, of Dallas, as a co-defendent. That portion of the case, however, was dismissed when the regional telephone company argued it had not violated the patent because it did not make the disputed switching equipment -- it had only bought it from AT&T.

But AT&T contends that Collins' patent was not valid.

Spokesman Curt Wilson said the Federal Patent Office is currently examining the patent in question in a separate proceeding at the request of both AT&T and Collins Licensing. "We think they will invalidate that patent and we won't have to pay," he said.

There is no firm time frame for the anticipated Patent Office ruling.

Wilson added that even if the patent is found by the government to have been valid, AT&T does not believe its equipment used Collins' discovery, and thus feels it did not infringe upon the patent.

"The jury found in our favor on seven of the original eight counts of the suit," Wilson said, "and on the remaining claim, awarded them $34 million, 70 times less than the amount they had originally sought."

We believe this suit is totally without merit," the spokesman asserted. "The patent is not valid -- and we expect the patent office to agree."

User "Bill Of Rights" Introduced January 23, 1992

TAMPA, FLORIDA.-- .The North American Directory Forum (NADF) introduced a "User Bill of Rights" to address security and privacy issues regarding entries and listings concerning its proposed cooperative public directory service. NADF members also approved continuing efforts on an experimental publish directory pilot at their eighth quarterly meeting.

The "User Bill of Rights" addresses the concerns of the individual user or the user's agent, and is in response to issues brought to the attention of the NADF.

Final plans were completed for the X.500 directory pilot scheduled to begin in the first quarter of this year. The pilot will be used by the NADF to validate its technical agreements for providing a publich directory service in North America. The agreements have been recorded in standing documents and include the services that will be provided, the directory schema and information sharing required to unify the directory. It will test the operation of X.500 in a large-scale, multi-vendor environment.

All NADF members are participating in the pilot. The members are AT&T, Bell Atlantic, BellSouth Advanced Networks, Bellcore representing US West, BT North America, GE Information Services, IBM, Infonet, MCI Communications Corp., Pacific Bell, Performance Systems International, US Postal Service and Ziff Communications Co. Joining the NADF at this meeting are Canada Post Corporation and DirectoryNet, Inc.

The NADF was founded in 1990 with the goal of bringing together major messaging providers in the U.S. and Canada to establish a public directory service based on X.500, the CCITT recommendation for a global directory service. The forum meets quarterly in a collaborative effort to address operational, commercial and technical issues involved in implementing a North American directory with the objective of expediting the industry's transition to a global X.500 directory.

This quarter's meeting was hosted by the IBM Information Network, IBM's value-added services network that provides networking, messaging, capacity and consulting services.

- -

USER BILL OF RIGHTS (for entries and listings in the Public Directory)

The mission of the North American Directory Forum is to provide interconnected electronic directories which empower users with unprecedented access to public information. To address significant security and privacy issues, the North American Directory Forum introduces the following "User Bill of Rights" for entries in the Public Directory. As a user, you have:

I. The right not to be listed.
II. The right to have you or your agent informed when your entry is created.
III. The right to examine your entry.
IV. The right to correct inaccurate information in your entry.
V. The right to remove specific information from your entry.
VI. The right to be assured that your listing in the Public Directory will comply with US or Canadian law regulating privacy or access information.
VII. The right to expect timely fulfillment of these rights.

- -

Scope of Intent - User Bill of Rights

The North American Directory Forum is a collection of service providers that plan to offer a cooperative directory service in North America. This is

achieved by interconnecting electronic directories using a set of internationally developed standards known as the CCITT X.500 series.

In this context, the "Directory" represents the collection of electronic directories administered by both service providers and private operators. When an entry containing information about a user is listed in the Directory, that information can be accessed unless restricted by security and privacy controls.

A portion of the Directory -- The Public Directory -- contains information for public dissemination. In contrast, other portions of the Directory may contain information not intended for public access. A user or user's agent may elect to list information in the Public Directory, a private directory, or some combination. For example, a user might publicly list a telephone number or an electronic mail address, and might designate other information for specific private use.

The User Bill of Rights pertains to the Public Directory.
Source: NADF, January 1992

Volume Four, Issue Thirty-Seven, File 13 of 14

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN              Phrack World News              PWN
PWN                                             PWN
PWN      Issue XXXVII / Part Three of Four      PWN
PWN                                             PWN
PWN     Compiled by Dispater & Spirit Walker    PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

THE RBOC'S GREED IS AIMED AT DESTROYING OUR BULLETIN BOARDS!

Computer Users See Threat In Costs November 5, 1991

By Martin Rosenberg (Kansas City Star)

"Southwestern Bell Plan Portends Changes, They Fear"

Some computer bulletin board operators in Missouri say they might have to shut down the increasingly popular computer networks if Southwestern Bell Telephone Company, succeeds in raising their rates.

Southwestern Bell says its only trying to fairly price its services by charging the bulletin board operators business rates instead of residential rates. The company is seeking approval for the changes from Missouri regulators.

Industry experts say the issue could be the opening volley in a broad campaign by telephone companies to change the way consumers and businesses pay for electronic communications.

Residential customers might one day have to pay more to use their personal computers and modems than they pay for voice communications, experts say. And businesses might have to pay more to use fax machines.

Southwestern Bell denied that it is attempting to change any rates other than those affecting a small number of data communications customers who should be switched to a flat business rate, more expensive than the residential rate.

The bulletin boards, frequently operated out of homes, allow users to exchange messages, advice and software programs. Many are free to use, and operators often get no revenue from them. Hundreds have formed across the state in the last few years.

Southwestern Bell's proposal is meant for only those who have set up a bulletin board through his or her personal computer. Not affected are computer users who merely access the bulletin board computer over telephone lines.

The proposal comes at a time when telephone companies' plans for information services have moved to center stage.

The U.S. Supreme Court (as already) cleared the way for seven regional telephone companies, including Southwestern Bell, to start providing information services. Those services could eventually compete with electronic bulletin boards, newspapers and data base operations such as CompuServe Inc. and Prodigy Services Co. (CompuServe is owned by H&R Block Inc. of Kansas City).

Revenues for telephone-delivered information in the United States amounted to an estimated $750 million last year and are projected to grow to $2 billion in 1992, according to industry sources.

Southwestern Bell's proposal, if approved, would take effect by mid-November.

Bulletin board operators are operating like businesses, said William Bailey, company district manager of rate administration for Missouri in St. Louis.

"Some customers on residential lines would more appropriately be on business lines," Bailey said.

Bailey said current business customers also would be affected. They would be allowed to switch to the flat business rate ($33.55 a month in metropolitan Kansas City) and avoid paying a higher "information terminal service" rate (currently $43.60 a month), he said.

Southwestern Bell mounted a similar effort to get bulletin boards under business rates in Texas. It later decided to allow free bulletin board services using three or fewer lines to continue to enjoy residential rates.

That was "an enormous mistake," Bailey said. Phone companies are unable to monitor whether a bulletin board is collecting money from users, he added.

Many Kansas City bulletin board operators are upset with Southwestern Bell's proposal.

"If they start charging business rates, some bulletin boards will shut down," said Lanny Conn, who operates a free bulletin board called SOLO-Quest.

Bill Hirt, who operates the Amiga Central bulletin board for Amiga computer users, said he would close down if he is charged the business rate. His bulletin board also is free to use.

Currently, about 200 personal computer users -- some as far off as Australia and Sweden - call his bulletin board, he said.

Conn and Hirt serve as spokesmen for the Greater Kansas City SysOps Association, made up of about 22 bulletin boards. (SysOps stands for system operators). Hirt estimates there are 100 bulletin boards in the city; most have been set up as hobbies.

Attorney Robin Martinez, who is representing the association, said that Southwestern Bell's proposal would hurt information-age pioneers.

"People running bulletin boards and people using them are on the cutting edge of the information age," he said.

Southwestern Bell wants to thin the ranks of bulletin board providers so there will be fewer competitors to its own offerings, he said.

"To a certain extent, they are trying to get a stranglehold on information services," Martinez said.

Bailey denied there is a link between his company's proposals and its own plans for information services.

"I'm not getting any direction from on high to do what I am doing," he said. "I'm really not aware what my company intends to do in terms of information services."

But William Degnan, a telecommunications consultant in Austin, Texas, said, "The majority of these folks (bulletin boards) are underpricing these services that Southwestern Bell would like to provide at a grander scale."

Degnan had advised the group of Texas bulletin board operators who had opposed Southwestern Bell's efforts to charge business rates there.

"I think Southwestern Bell is concerned that (it) won't be able to sell what other people are giving away," Degnan said.

Martha Hogerty, public council representing consumers in Missouri, said after reviewing Southwestern Bell's filing, "This looks like anybody with a modem would have to be on a business rate."

Most regional Bell telephone companies are now developing strategies for

offering information services.

Phone companies may soon try to get customers to pay a measured rate for data communications, said Howard Anderson, president of the Yankee Group of Boston. Under such a system, the monthly cost of data communications would increase the longer you are connected during the month -- like a running taxi meter.

A change to metered rates would be reasonable and enable telephone companies to increase revenues as usage and expenses mount, he said.

The average residential customer uses the phone 21 minutes a day, while a customer with a personal computer and modem uses a phone line an average of 62 minutes a day, Anderson said.

Anderson predicted that telephone companies may decide to offer customers high-speed data communications for a rate higher than voice communications. Usage above a fixed number of hours would increase the size of the monthly phone bill, he said.

To encourage use of the new line, phone companies may take steps to lower the quality of standard lines so that they will not cleanly carry electronic information, Anderson said.

Bailey disagreed, saying Southwestern Bell has no plans to introduce measured service for voice or data communications.

And, he said, "I know of no plans to degrade our service to migrate customers >from one service to another."

SW Bell Tariff Called Threat to Computer Bulletin Boards November 18, 1991

By Robert Sanford (St. Louis Post-Dispatch)

A proposal by Southwestern Bell Telephone Co. to revise a tariff for telephone use has brought protests from owners of personal computers who use phone lines to operate bulletin board services for other computer owners.

The bulletin board operators contend that their members - by and large - operate bulletin boards as a hobby and not a business. And they contend that the change suggested by Bell is part of an effort by the phone company to make them pay business phone line rates rather than residential rates.

Bulletin boards are computers with modems that can be accessed by other computers with modems. The "bulletin boards" contain information that can be passed to other computers - information of any sort, from cooking recipes to games to automobile tips to computer programming.

Hobby bulletin board users have common interests, said Jim Harre, coordinator of a bulletin board network called Network 100. "You could say that bulletin board users are somewhat similar to amateur radio operators. They are people using computers to communicate. They serve a function like a bulletin board at a supermarket. They pass on information.

The operators see the Bell proposal as a threat to all bulletin boards. Increased costs would simply force some hobby boards out of existence."

A list of several networks in the St. Louis area shows there are about 250 bulletin boards in the area, said Bob Schmedake, a system operator, or "sysop", as they call themselves. It is estimated that there may be that many in the Kansas City area. So there are several hundred across the state. There are 16,000 bulletin boards listed worldwide.

Although the tariff proposal has brought the issue of residential vs. business rates to the forefront in discussions among Missouri sysops, the proposal does not suggest any sort of residential rate change. The proposal suggests that some users of a different sort of service called Information Terminal Service should be allowed to change to flat business rate.

Generally, the ITS rate is $43.65, the flat business rate is $33.55 and the residential rate is $11.35.

A definition in the phone company's existing tariffs says in part that a line used "more as a business than of a residence nature" should be billed at a business rate, said William Bailey, Southwestern Bell's district manager for rate administration in Missouri.

A "business nature" could be said to be present if the line is advertised in any way, he said.

But the nature of the growth of bulletin boards has been that computer owners added modems to personal computers in the home and began communicating with others by computer, using residential line, the sysops say. Most always have thought of bulletin boards as a hobby, they say. Though there may be some charges for access to bulletin boards, nobody makes any money at it, they said.

Bailey said that the phone company does not know how many sysops there are using residential lines and the company has no formal plan to try to determine how lines are being used.

Bailey attended a meeting in Kansas City that also was attended by John Van Eschen, assistant manager for telecommunications for the Missouri Public Service Commission, and about 150 sysops.

The meeting was described later as being "testy" at times and the outcome was that the sysops and the phone company agreed to disagree. Users contended that bulletin boards are a public service offering information and that rate increases could force some to shut down.

"The users want to be billed as residential", Van Eschen said. "An avenue toward getting that would be to file a formal complaint against Bell. That could lead to written testimony and a hearing."

He said there is a complaint on file now charging that Bell wanted to change user's rate from residential to business and there was talk at the meeting about some sort of legal action.

Van Eschen said the PSC is continuing to study the question and has made no recommendation. The effective date for application of a ruling would be December. 15.

Some sysops, Harre among them, suggest that the phone company might be interested in reducing the number of bulletin boards because the company has plans to enter the information services business itself and may see bulletin boards as potential competitors. The Supreme Court recently upheld a ruling that allowed the Baby Bell companies to enter information services.

Bailey said he was not aware of what the company plans to do in the information services business.

Phone Companies Eyeing Higher Rates for BBSes November 18, 1991

By Steve Higgins (PC Week)(Page 173)

The shoestring bulletin-board service could be a thing of the past if the major telephone companies have their way.

Regional operating companies such as U.S. West Inc., Southwestern Bell Corp. and Southern Bell Telephone & Telegraph Co. are maneuvering to raise the cost of doing business for the more than 40,000 operators of dial-in bulletin boards in the United States, those operators say.

The bulletin board services (BBSs), whose offerings run the gamut from technical support to discussions on exotic birds, could be crippled or killed off completely by higher installation costs and monthly line charges that, in

some cases, would double the current rates.

"If the telephone companies were to raise the operating costs, we would have to pass that on to users," said Kevin Beherens, operator of Aquilla BBS, a distributor of shareware in Aurora, Ill.

While attempts to up the ante have thus far been rebuked by overwhelming opposition from BBS users, a proposal by Southwestern Bell that could make it easier for the company to crack down on BBS operators who are paying low, residential phone-line rates is up for review this month.

"We have a tariff for business customers. Bulletin-board service operators should be paying that rate," said David Martin, a spokesman for Southwestern Bell in St. Louis. "We don't now have an organized program to move bulletin-board providers to that rate."

The companies region covers five states in the Midwest and the southern United States, but the proposal would take effect only in Missouri. If approved by Missouri regulators, it could more than double the monthly rate for operators of bulletin-board systems.

Business data-line rates average $18 to $45 per month nationally, while residential rates average $7 to $20 per month.

In addition, a federal judge's ruling in October that frees the telephone companies to operate their own bulletin-board services could make price hikes even more tempting. Because of the federal ruling, analysts say, the phone companies' interest in raising costs for BBS operators extends beyond extracting more revenue.

"The phone companies want to put up electronic Yellow Pages...[which] in itself [is] not a bad thing," said Jack Rickard, editor of Boardwatch, a monthly magazine for BBS users that is published in Lakewood, Colorado. "But the mentality seems to be to stop anything else."

COMPETITORS ABOUND

Should they unveil their own on-line services, the phone companies will find a prodigious installed base with which to compete. In addition to the garage BBS operations, nearly 40 of the top 100 PC software companies are exploiting the low expense and wide reach of bulletin boards to provide customer support, according to Soft*letter, an industry newsletter based in Watertown, Massachusetts.

"We are just now starting to see business use bulletin-board services," said Jim Harrer, president and CEO of Mustang Software Inc., a vendor of communications software and a bulletin-board service operator located in Bakersfield, Calif. "It would cripple them if [tariffs] got in the way."

If that becomes the case, observers say, some system operators might try to dodge the new tariff by disguising their operations as personal telephone lines. In fact, some operators are reportedly trying that tactic already.

"I've heard of one guy who was who was trying to convince the phone company that he has five kids" who needed separate phone lines, Mustang Software's Harrer said.

Increased costs could also affect the large bulletin-board operators, such as Prodigy Services Co. and CompuServe Inc., particularly if coupled with the emergence of bulletin boards maintained by telephone companies.

"It is not going to push them out of business," said Boardwatch's Rickard, "but [Prodigy and CompuServe] are also affected."

Southwestern Bell's Scorched Earth Policy For Bulletin Boards December 1991

Taken from BOARDWATCH Magazine

Throughout the debate on whether to allow the Regional Bell Operating Companies (RBOC) into the information business, opponents warned that the RBOC would use their monopoly position to unfairly eliminate competition. And throughout this debate, the RBOC piously denied they would ever do anything anti-competitive. Judge Greene warned in clear and ringing terms that their history indicated they would and denied them repeatedly the freedom to compete in information services over the course of the seven years since divestiture.

Using millions in rate-payers funds, the RBOC lobbied and appealed through every venue in government and finally found an appeals court who directed Judge Greene to reconsider his stand.

Forced to lift the ban on information content, Greene issued a stay on his ruling pending appeals by the opposition. In an October 7 decision by the appeals court, even the stay was overturned freeing the bells over night to operate their own online services.

The ink had not completely dried on the document when they levied their opening shot. Southwestern Bell Telephone, with a history of BBS harassment going back to the mid-80s already under their belt, was the first out of the gate. In October, they filed a tariff revision asking that ALL electronic bulletin boards, whether operated for profit or as a hobby, be classified as Information Terminal Services and not only forced to pay higher business rates, but specifically prevented from using existing business measured service tariffs to reduce their telephone bills. The tariff was filed October 7, 1991 as a proposed revision to Missouri Local Exchange Tariff, P.S.C. Mo. No. 24 and P.S.C. Mo. No. 35, General Exchange Tariff, Section 17, Rules and Regulations Applying to all Customer's Contracts.

Currently, the basic line charge for businesses in the Kansas City area is $33.55 monthly--about twice the residential rate. And the Information Terminal Rate is actually higher yet at $43.60 monthly. While the tariff modification is specifically aimed at BBS operators, the wording of the tariff would seem to include anyone who uses a modem or fax machine on a telephone line.

Southwestern Bell has a history of animosity with regards to bulletin board operations. The company announced their own SOURCELINE gateway data service in Houston in 1988 and delivered letters to hundreds of Houston bulletin boards in October of that year demanding they pay business rates for their residential telephone lines. A group of local system operators operating under the banner of COSUARD took their case to the Texas Public Utilities Commission, charging predatory practices, anti-competitive actions, and discrimination against the hobby BBS community.

Southwestern Bell, concurrent with the grandiose failure of their own SOURCELINE gateway service, settled with the group in January 1991. All BBS in the Houston area operating on three or fewer lines and not seeking subscriber support are classified as hobby BBS and continue to qualify for residential telephone service.

Hobby bulletin boards are really the issue. Most commercial or subscription bulletin board systems already pay business telephone rates for their systems. However, most opt for a type of business classification referred to as "totally measured service." Virtually all RBOC offer a reduced basic rate in exchange for the right to meter local calls -- usually at two or three cents per minute. Since most bulletin boards make few outbound calls -- most of the activity is incoming--the totally measured service, even in a business classification, is only a few dollars more than residential telephone service. SWB in their filing, if approved, would effectively double the telephone charges for any BBS in the state of Missouri overnight.

Kansas City system operators have banded together to form a non-profit organization titled the Greater Kansas City Sysops Association (GKCSA) to fight the proposed change. At a November 14th public hearing in Kansas City, nearly 150 operators and callers showed up to protest the action and the MPSC agreed to delay implementation of the new rate until December 15th. SWB had originally sought to apply the rates effective November 15.

According to GKCSA attorney Robin Martinez, the group will be filing a legal petition asking the MPSC to rule that all hobby BBS operating on residential premises be allowed the lower residential rate classification. The GKCSA contends in its petition that Southwestern Bell Telephone is acting in a predatory and anti-competitive manner in seeking to eliminate any perceived competition to their own planned information services in Missouri.

GKCSA president Scott Lent predicts that if Southwestern Bell gets their way, it will be the end of the free hobby BBS in the state -- which is just what the telephone company wants. And he predicts that if SWB wins in Missouri, the other RBOC won't be far behind with tariffs of their own to eliminate the competition of underpriced information services represented by the free BBSs.

William Bailey, company district manager of rate administration for Missouri, makes no apologies for the company's approach. At the Kansas City meeting he admitted that the charge will have no significant impact on company revenues, but denied that it was in any way connected to their entry into information services and avowed that he wasn't informed what the company's plans were in information services. He claimed their only goal was "fairness" in that modem users tied up the system longer than voice callers and should pay more. He could not comment on the coincidence of SWB filing for the tariff within a week of the appeals court decision.

Computer Phone-Fee Plan Angers Many December 8, 1991
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

By Christine Bertelson (St. Louis Post-Dispatch)

"Costs May Triple For Electronic Bulletin Boards"

For Barbara Clements, the electronic bulletin board she operates on her home computer in south St. Louis County is far more than a hobby. It is her only window on the world.

Clements, 43, has severe cerebral palsy, which prevents her from walking or using her hands. Her garbled speech is difficult for many people to understand in public and impossible to comprehend on the telephone, she says.

But by sitting at the keyboard and using a head wand, Clements is able to use her modem and computer to communicate with a growing network of other computer hobbyists.

The computer network has given her a freedom and social life she is loath to lose.

"Six years ago, before I got my modem, I was a total hermit," Clements said in an interview at her home.

"My privately run bulletin board system is strictly social for my sanity. I am an equal human being on any bulletin board system because people cannot see my disability and they cannot hear my garbled speech. This makes it easier to make friends."

Clements is one of hundreds of computer hobbyists statewide who would be affected by a proposal by Southwestern Bell Corp. to charge bulletin board operators business rates instead of residential rates for telephone hookups to their terminals.

The proposal would affect not only disabled people such as Clements who see the network as a lifeline to the outside world.

The bulletin boards have become increasingly popular with computer hobbyists in the general population as well - as a way to exchanging information about computers and various other interests.

Those involved from teen-age "computer hackers" to adults trading recipes to singles looking for dates.
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Hundreds of electronic bulletin boards have been added to the network across Missouri the past few years. In the St. Louis area, more than 200 are in place. Only operators of the boards would be affected by the proposed rate boost; hundreds of others who phone into them would not be covered.

The company announced the plan several weeks ago. The issue is expected to soon be before the Missouri Public Service Commission, which regulates utility rates in the state.

The telephone company says it is only trying to price its services fairly, noting that computer chitchat often lasts longer than telephone calls. Tying up telephone lines increases Bell's operating costs, a spokesman said.

Robin Martinez, a lawyer from Kansas City representing computer hobbyists there, said he plans to file a complaint this week, calling for a public hearing on the issue.

William Bailey, Southwestern Bell's district manager of rate administration for Missouri, said the company considers electronic bulletin boards operated by people such as Clements as businesses.

"If a customer acts as a business, by advertising and other things, we could charge a business rate," Bailey said. "We charge business rates to clubs and fraternities. One reason we price businesses higher is to keep residential rates lower."

Electronic bulletin boards, frequently operated from homes, function as a meeting place, their operators say.

Many are free to use, and operators often get no income from them.

Each has its on name, reflecting the personality of its "sysop" or system operators. Clements dubbed hers, appropriately, "Barb's Outlook Window."

One of Clements' electronic acquaintances is John Brawley Jr. of Eureka, known by his computer handle "The Wanderer."

The two met three months ago on her bulletin board and now regularly talk by computer about subjects from the weather to Clement's cerebral palsy to Brawley's ideas on the impact of quantum mechanics on religious concepts.

Brawley is concerned that Bell's proposal would effectively gag Clements. But, he said, there is a broader issue involved also. Charging the higher rates would restrict the free flow of information, he said.

Bailey said the principle at stake is not freedom of speech, but merely the definition of what is a business and what is not.

The U.S. Supreme Court recently cleared the way for regional telephone companies, including Southwestern Bell, to provide information services that could eventually compete with electronic bulletin boards, newspapers and data base operators.

Revenue for telephone-delivered information in the nation was estimated at $750 million last year and projected at $2 billion next year, industry sources said.

Martinez, the lawyer for the Kansas City bulletin users, estimated that Southwestern Bell could take in $8 million more a year by charging the business rates in question. Bailey would not confirm that figure.

Once computer hobbyists file a formal complaint with the state commission, Bell would have 30 days to respond. If the issue is not resolved privately, the commission may hold a public hearing, said agency spokesman Kevin Kelly.

In the meantime, Clements said she has written to the company and is eager to testify at a hearing.

Agreement Nears For Phone Company And Missouri BBS Sysops February 14, 1992

Taken from Newsbytes

The report from Kansas City is that Southwestern Bell phone company is nearing an agreement with local operators of computer bulletin board systems in dispute over the company's charging BBSes business rates. The pact seems to center on language in a new tariff plan.

Communications Daily newsletter this week quoted attorney Robin Martinez, representing the sysops, as saying the proposed agreement calls for BBSes to be exempt from business rates if they meet certain conditions.

One of the conditions is that the boards must be located in residences. Exempted BBSes also must not charge for access, must not advertise and must have fewer than five phone lines.

Martinez says the last stumbling block in the agreement is coming up with a workable definition for "BBS" for the tariff language.

Final Notes

There are still some problems to be worked out in the Missouri/Southwestern Bell situation, but meanwhile, there are other similar problems going on with C&P (Bell Atlantic) Telephone in Virginia and US West Telephone in Oregon.

Our electronic rights and freedoms that we have enjoyed for oh so many years are in jeopardy because of the greed of the Regional Bell Operating Companies.

Support our Congress by supporting S 2112 and HR 3515!

More details in Phrack 38.

PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN PWN
PWN Phrack World News PWN
PWN PWN
PWN Issue XXXVII / Part Four of Four PWN
PWN PWN
PWN Compiled by Dispater & Spirit Walker PWN
PWN PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN

Computer Espionage: Can We Be Compromised By The Internet? December 1991

Extracted from Security Awareness Bulletin

The advent of computer networks linking scientists and their research institutions vastly complicates any effort to identify Soviet scientific espionage. For example, foreign travel may become less important, as computers become more directly interconnected, allowing scientists anywhere in the world to talk to each other -- and, in some cases to access information in data bases at Western academic and defense-related institutions.

This capability has been available for some time, but in 1989 the USSR took an important step toward increasing the breadth and availability of access, by applying (with Poland, Czechoslovakia, Hungary, and Bulgaria) to be connected to the European Academic Research Network (EARN). Approval of the application in April 1990 provided Soviet and East European users access far beyond simply a link to computers throughout Western Europe. Through EARN, the Soviets would be connected to Internet, a US network serving defense, research, and academic organizations worldwide.

A number of threats are inherent in the trend toward computer linkage. The most obvious is the increased ease with which a Soviet can discuss professional matters with Westerners working on similar projects. A user also can put out a blanket request for information on any subject, and it may not always be obvious that the requestor is working for the USSR. In addition, the Soviet Academy of Sciences can use a computer network to issue general invitations to conferences -- in hopes that the responses will identify untapped research institutions or individual scientists that later can be targeted for specific information.

Access to data in the computers connected to a network normally is controlled, so that specific files can be read only by authorized users. However, the Soviets have demonstrated that an innovative "hacker" connected to computers containing sensitive information can evade the access controls in order to read that information. In the "Hannover Hacker" case, for example, the Soviet intelligence services used West German computer experts to access US restricted data bases, obtaining both software and defense-related information.

Waging War Against War Dialing November 27, 1991

By Edmund L. Andrews (New York Times)
Special Thanks: Dark Overlord

WASHINGTON -- Riding a wave of popular annoyance over telephone sales calls, Congress approved and sent to President Bush a bill that would ban the use of automated dialing devices that deliver pre-recorded messages to the home. The measure would also allow consumers to block calls from human sales-people by placing their names on a "do not call" list.

The bill, which passed on voice votes in both the House and Senate, was supported by both Democrats and Republicans, some of whom have recounted their own aggravations with unsolicited sales calls.

Although the White House has expressed concerns about what it views as unnecessary regulation, the President has not threatened to veto the bill.

The measure, which combines provisions from several separate measures passed previously by both chambers of Congress, bans the use of autodialers for calling most individual homes. The few exceptions would be when a person has explicitly agreed to receive such a call or when the autodialer is being used to notify people of an emergency.

When autodialers are used to call businesses, they would be prohibited from reaching more than two numbers at a single business.

Many states have already passed laws that restrict autodialers, including about a dozen states that ban them altogether and about two dozen others that restrict their use in various ways.

The state laws, however, do not stop a company from using an autodialer in an unregulated state to call homes in state with regulations.

In an attempt to curb telemarketing by human sales representatives, the measure would instruct the Federal Communications Commission to either oversee the creation of a nationwide "do not call" list or issue rules ordering companies to maintain their own lists.

The bill would allow people who placed their names on such a list to file suits is small claims courts against companies that persisted in calling. The suits could seek up to $500 for each unwanted call, up to a maximum of three calls >from a single company.

Finally, the bill would ban unsolicited "junk fax" messages, which are advertisements transmitted to facsimile machines.

"This is a victory for beleaguered consumers, who in this piece of legislation have their declaration of independence from junk faxes and junk calls," said Rep. Edward J. Markey, D-Mass., the measure's principal sponsor in the House.

Companies that make or use autodialers glumly predicted that the measure would put them out of business and would hurt small advertisers the most.

"I think it will put us out of business," said Mark Anderson, owner of the Leshoppe Corp., a New Orleans concern that uses about 160 machines for clients who sell everything from tanning products to health insurance. "What people don't understand is that a lot of mom-and-pop operations use electronic marketing, and use it successfully."

Ray Kolker, president of Kolker Systems, the largest maker of autodialers, echoed those views. "Passage of this bill demonstrates that Congress just isn't as concerned about the economy as they think they are," he said. "This will destroy a multibillion-dollar business."

Telemarketing has surged in recent years, as the cost of long-distance telephone service has plunged and as consumers have become deluged by floods of catalogues they do not read and envelopes they do not open.

According to congressional estimates, the volume of goods and services sold through all forms of telephone marketing has increased from about $72 billion in 1982 to $435 billion in 1990. Over all, an estimated 300,000 people are employed in some facet of telephone marketing.

Autodialers, which can each make about 1,500 calls a day, have become one of the most efficient but disliked forms of telemarketing. By one estimate, 20,000 autodialers are in operation at one time, with the capacity of making more than 20 million calls in a single day.

During hearings on the issue earlier this year, Sen. Daniel K. Inouye, D-Hawaii, noted irritably that he had been summoned to the telephone only to hear a recorded sales message about winning a trip to Hawaii.

The legislation was not opposed by all companies involved in telephone sales. Many marketing experts have long deplored the use of autodialers as a sales tool, arguing that they are counter-productive because they generate more

irritation than sales interest.

The Direct Marketing Association, a trade group, has expressed cautious support for the legislation and already maintains its own, voluntary "do not call" list.

Beyond simply annoying people at home, the autodialers have been known to tie up telephone paging networks and the switchboards of hospitals and universities, and to call people on their cellular telephones.

But it remains unclear how effective the "do not call" lists would be in practice, because the two options available to the FCC differ greatly.

A national list maintained by the government would effectively protect consumers from all unwanted sales calls. But a requirement that each company maintain its own list would be much more limited, because people might have to call each company to be placed on its individual list.

Congressional aides noted that the measure passed Wednesday strongly implied that the FCC should set up its own list, because it provides two pages of detail on just how such a list should be created.

Foreign Guests Learn America Is Land Of The Free December 2, 1991
~~~~~~

Excerpted from the Orlando Sentinel

"Merry Christmas From BellSouth!"

A telephone computer glitch gave dozens of foreign travelers at downtown Orlando hotel early Christmas presents Saturday and Sunday.

The giving began when a guest at the Plantation Manor, an international youth hotel across from Lake Eola, discovered that pay phones were allowing free long-distance calls to virtually anywhere in the world.

As the news spread, the four public phones, which are normally deserted at the hotel, were busy non-stop until Sunday afternoon,when Southern Bell discovered the problem and dispatched technicians to shut off long-distance service.

Roger Swain, a clerk at Plantation Manor, said the discovery was made by accident.

"One of our guests said he tried to call Houston, Texas, from the second floor," Swain said. The operator told him he didn't need to use coins because the phone was not listed as a public phone. He was on the phone for 40 minutes, and they didn't charge him.'

A spokesman for AT&T, which handles long distance for some of Southern Bell's phones, said the problem seemed to be with a Southern Bell computer.

"Our equipment is working fine," said Randy Berridge, AT&T spokesman. "If it's a Southern Bell problem, they would bear the costs.'

It's possible Southern Bell recouped some money: It still cost 25 cents for a local call.

"This is a drop in the ocean to them," one English traveler said of the phone company, which had just covered the cost of his call home at the Sunday rate of $21.74 for each half hour."

8th Chaos Computer Congress December 27-29, 1991
~~~~~~~~~~~~~~~~~~~~~~~~~~

by Klaus Brunnstein

Special Thanks: Terra of CCC

On occasion of the 10th anniversary of its foundation, Chaos Computer Club (CCC) organized its 8th Congress in Hamburg. To more than 400 participants (largest participation ever, with growing number of students rather than teen-age scholars), a rich diversity of PC and network related themes was offered, with significantly less sessions than before devoted to critical themes, such as phreaking, hacking or malware construction. Changes in the European hacker scene became evident as only few people from Netherlands (e.g. Hack-Tic) and Italy had come to this former hackers' Mecca.

Consequently, Congress news are only documented in German. As CCC's founding members develop in age and experience, reflection of CCC's role and growing diversity of opinions indicates that teen-age CCC may produce less spectacular events than ever before.

This year's dominating theme covered presentations of communication techniques for PCs, Ataris, Amigas and Unix, the development of a local net as well as description of regional and international networks, including a survey. In comparison, CCC '90 documents are more detailed on architectures while sessions and demonstrations in CCC '91 (in "Hacker Center" and other rooms) were more concerned with practical navigation in such nets.

Phreaking was covered by the Dutch group HACK-TIC which updated its CCC '90 presentation of how to "minimize expenditures for telephone conversations" by using blue boxes and red boxes, and describing available software and recent events. Detailed information on phreaking methods in specific countries and bugs in some telecom systems were discussed. More information (in Dutch) was available, including charts of electronic circuits, in several volumes of Dutch "HACKTIC: Tidschrift voor Techno-Anarchisten" (news for techno-anarchists).

Remark #1: Recent events (e.g. "Gulf hacks") and material presented on Chaos Congress '91 indicate that the Netherlands emerges as a new European center of malicious attacks on systems and networks.

Among other potentially harmful information, HACKTIC #14/15 publishes code of computer viruses (a BAT-virus which does not work properly.

Remark #2: While few Netherland universities devote research and teaching to security, Delft university at least offers introductory courses into data protection.

Different from recent years, a seminar on Computer viruses (presented by Morton Swimmer of Virus Test Center, University of Hamburg) as deliberately devoted to disseminate non-destructive information (avoiding any presentation of virus programming). A survey of legal aspects of inadequate software quality (including viruses and program errors) was presented by lawyer Freiherr von Gravenreuth.

Some public attention was drawn to the fact that the "city-call" telephone system radio-transmits information essentially as ASCII. A demonstration proved that such transmitted texts may easily be intercepted, analyzed and even manipulated on a PC. CCC publicly warned that "profiles" of such texts (and those addressed) may easily be collected, and asked Telecom to inform users about this insecurity; German Telecom did not follow this advice.

Besides discussions of emerging voice mailboxes, an interesting session presented a C64-based chipcard analysis systems. Two students have built a simple mechanism to analyze (from systematic IO analysis) the protocol of a

German telephone card communicating with the public telephone box; they described, in some detail (including an electronmicroscopic photo) the architecture and the system behavior, including 100 bytes of communication data stored in a central German Telecom computer. Asked for legal implications of their work, they argued that they just wanted to understand this technology, and they were not aware of any legal constraint. They have not analyzed possibilities to reload the telephone account (which is generally possible, due to the architecture), and they did not analyze architectures or procedures of other chipcards (bank cards etc).

Following CCC's (10-year old charter), essential discussions were devoted to social themes. The "Feminine computer handling" workshop deliberately excluded men (about 25 women participating), to avoid last year's experience of male dominance in related discussions. A session (mainly attended by informatics students) was devoted to "Informatics and Ethics", introducing the international state-of-discussion, and discussing the value of professional standards in the German case.

A discussion about "techno-terrorism" became somewhat symptomatic for CCC's actual state. While external participants (von Gravenreuth, Brunnstein) were invited to this theme, CCC-internal controversies presented the panel discussion under the technical title "definition questions". While one fraction wanted to discuss possibilities, examples and dangers of techno-terrorism openly, others (CCC "ol'man" Wau Holland) wanted to generally define "terrorism" somehow academically, and some undertook to describe "government repression" as some sort of terrorism. In the controversial debate, a few examples of technoterrorism (WANK worm, development of virus techniques for economic competition and warfare) were given.

Another AT&T 800-Number Outage

December 16, 1991

By Dana Blankenhorn (Newsbytes)

BASKING RIDGE, NEW JERSEY -- AT&T suffered another embarrassing outage on its toll-free "800" number lines over the weekend, right in the middle of the Christmas catalog shopping season.

Andrew Myers, an AT&T spokesman, said the problem hit at 7:20 PM on December 13 as technicians loaded new software into computers in Alabama, Georgia, and New York. The software identifies and transfers 800 calls, he said. A total of 1.8 million calls originating in parts of the eastern U.S. were impacted, the company said.

Service was restored after about one hour when technicians "backed off" the patch and went back to using the old software. Programmers are now working on the software, trying to stamp out the bugs before it's reloaded. "Obviously we don't like it when a single call doesn't get through, but I wouldn't consider this a serious problem," Myers said. The problem was reported to the Federal Communications Commission over the weekend, and to the press the next day.

The latest problem continues a disturbing trend of AT&T service outages in the Northeast. Worse, all the problems have had different causes -- power problems, switch software problems, and cable cuts caused previous outages.

US Congress Sets Up BBS For Whistle Blowers

December 16, 1991

By Dana Blankenhorn (Newsbytes)

WASHINGTON, D.C. -- U.S. Congressman Bob Wise and his House Government Operations subcommittee on government information, justice and agriculture have opened a bulletin board service for government whistle-blowers.

Wise himself is the system operator, or sysop, of the new board. Newsbytes contacted the board and found it accepts parameters of 8 bit words, no parity, and 1 stop bit, known as 8-N-1 in the trade, and will take calls from a standard 2400 bit/second Hayes- compatible modem.

Whistle-blowers are employees who tell investigators about wrong- doing at their companies or agencies, or "blow the whistle" on wrong-doing. Wise said that pseudonyms will be accepted on the BBS -- most private systems demand real names so as to avoid infiltration by computer crackers or other abusive users. Passwords will keep other users from reading return messages from the subcommittee, Wise added. The committee will check the board daily and get back to callers about their charges. The board is using RBBS software, a "freeware" package available without license fee.

The executive branch of the U.S. government uses a system of inspectors general to police its offices, most of whom have telephone hotlines for whistle-blowers and accept mail as well. But the inspectors expect whistle-blowers to collect evidence at work, which could get them in trouble. And efforts to contact the whistle-blower by an inspector general representative can identify them to wrongdoers. Theoretically, calls from Congressional staffers will be seen by the bad guys as typical annoying oversight calls.

Press Contact: Rep. Bob Wise
202-224-3121
202-225-5527 BBS

NIST Extends Review Deadline for Digital Signature December 16, 1991

By John McCormick (Newsbytes)

WASHINGTON, DC -- NIST, the National Institute of Standards and Technology (formerly the Bureau of Standards) has taken the unusual step of extending the review period for the controversial digital signature standard which the agency proposed at the end of August.

The normal 90-day comment period would already have ended, but the NIST has extended that deadline until the end of February - some say because the agency wishes to tighten the standard.

NIST spokespersons deny that there was any need to modify the proposed standard to increase its level of security, but James Bidzos, whose RSA Data Security markets a rival standard, says that the NIST's ElGamal algorithm is too weak and is being promoted by the government because the National Security Agency feels that it can easily break the code when necessary.

The new standard is not a way of encrypting messages themselves; that is covered by the existing DES or Data Encryption Standard. Rather, the DSS or Digital Signature Standard is the method used to verify the "signature" of the person sending the message, i.e., to make certain that the message, which might be an order to transfer money or some other important item, is really >from the person who is authorized to send such instructions.

As Newsbytes reported back in July, the NSA and NIS had been charged with developing a security system nearly four years ago. The recently announced ElGamal algorithm was previously due to be released last fall, and in the meantime the RSA encryption scheme has become quite popular.

At that time, NIST's deputy director, Raymond G. Kammer, told the Technology and Competitiveness Subcommittee of the House (U.S. House of Representatives) Science, Space and Technology Committee that the ElGamal encryption scheme, patented by the federal government, was chosen because it would save federal agencies money over the private RSA encryption and signature verification scheme.

Interestingly enough, the only company that currently markets an ElGamal DS system is Information Security Corp., 1141 Lake Cook Rd., Ste. D, Deerfield, IL 60015, a company that fought and won a bitter court battle with RSA over the right to market RSA-based encryption software to the federal government. That was possible because RSA was developed at MIT by mathematicians working under federal grants.

ISC's $249.95 Secret Agent, which uses the ElGamal algorithm, was released at last year's Federal Office Systems Expo in Washington. ElGamal is a public key system that can be used just like the RSA system but differs from it in significant theoretical ways.

ISC's CEO and president, Thomas J. Venn, has told Newsbytes that the ElGamal system is highly secure, but the ElGamal algorithm is quite different from that of the RSA system, deriving its security from the difficulty of computing discrete logarithms, in finite field, instead of using RSA's very different

method of factoring the products of two prime numbers.

RSA has fought back by posting a prize for anyone who can crack the RSA scheme. To take a stab at it, send a self-addressed stamped envelope to RSA Data Security, Inc., 10 Twin Dolphin Dr., Redwood City, CA 94065, for the RSA list and the rules. Those with access to Internet e-mail can send a request to challenge-info@rsa.com.

PWN Quicknotes
~~~~~~~~~~~~~~~

1. Computer bulletin boards aren't just for dweeby cyberpunks anymore -- at least not in San Francisco. Entrepreneur Wayne Gregori has created SF Net, a decidedly socialble computer network that links up patrons of the city's dangerously hip cafe's. From the Lower Haight to south of Market Street, high-tech trendies are interfacing over cappuccino. All you have to do is buy a ticket from the cafe>, enter a number into an on-site computer and begin your techno-chat at $1 per 15 minutes. The next Gregori test site is Seattle, Washington. (Newsweek, December 2, 1991)

---

2. The (November 29, 1991 issue of) San Jose Mercury News reported that the San Mateo, California 911 system was brought to it's knees because of a prank <but not by any computer hacker or phone phreak>.

   It seems that a disc jockey at KSOL decided to play a recent MC Hammer record over and over and over... as a prank. Listeners were concerned that something had happened to the personnel at the station, so they called 911 (and the police department business line). It seems that a few hundred calls in forty five minutes or an hour was enough to jam up the system. There was no report in the newspaper of any deaths or injuries to the overloaded system.

   The DJ didn't want to stop playing the record (claiming First Amendment rights), but did insert an announcement to not call the police.

---

3. Jean Paul Barrett, a convict serving 33 years for forgery and fraud in the Pima County jail in Tuscon, Arizona, was released on December 13, 1991 after receipt of a forged fax ordering his release. It appears that a copy of a legitimate release order was altered to bear HIS name. Apparently no one noticed that the faxed document lacked an originating phone number or that there was no "formal" cover sheet. The "error" was discovered when Barrett failed to show up for a court hearing.

   The jail releases about 60 people each day, and faxes have become standard procedure. Sheriff's Sergeant Rick Kastigar said "procedures are being changed so the error will not occur again." (San Francisco Chronicle, December 18, 1991, Page A3)

---

4. AT&T will boosted it's rates on direct-dial, out-of-state calls on January 2, 1992. The increase, to affect weekday and evening calls, would add about 8 cents to the average monthly long-distance bill of $17 and about $60 million to AT&T'd annual revenue. (USA Today, December 23, 1991, Page B1)

---

5. The following was in the AT&T shareholders quarterly, and is submitted not as a commercial solicitation but because somebody might be interested.

   A colorful 22-by-28-inch poster that traces the development of the telephone from Bell's first model to the latest high-technology feature phone can be purchased for $12. To order, send a check to Poster, AT&T Archives, WV A102, 5 Reinman Road, Warren, NJ 07059-0647. (Telephone 908-756-1590.)"

   (Special Thanks: The Tone Surfer)
~~~~~~~~~~~~~~~

---

6. Word has it that the normal toll-free number blue-box is now DEAD in Norway. According to some information received by Phrack, the toll-free numbers got switched onto the regular phone network in the United States, which you can't phreak the same way. (Special Thanks: Nosferatu)

---

7. In case you've been trying to call Blitzkreig BBS and been unable to connect with it, Predat0r is moving his board into the basement. He said the board would be back up as of February 1st. He also said that master copy of TAP #106 is finished, but he is a year behind on updating his mailing list. Predat0r said that making the copies was no problem but that with the influx of subscribers he was going to have to enlist local help to get the database updated. He also said that if someone paid for ten issues they will get ten issues. (Special Thanks: Roy the Tarantula)

---

8. There is a new science fiction book about called "Fallen Angels" by Larry Niven. The basis for the book is this: The United States government has been taken over by religious fanatics and militant environmentalists. Soon the United States is an Anti-Technological police state. Two astronauts are shot down over the United States and are on the run. They are on the run from various government agencies such as the (Secret Service like) Environmental Protection Agency. Nivin's wild imagination provides for a great deal of humor as well as some things that are not funny at all, due to the fact that they hit just a little to close to home.

   The story also mentions the Legion of Doom and The Steve Jackson Games raids. In the "acknowledgments" section at the rear of the book the author has this to say, "As to the society portrayed here, of course much of it is satirical. Alas, many of the incidents --- such as the Steve Jackson case in which a business was searched by Secret Service Agents displaying an unsigned search warrant --- are quite real. So are many of the anti-technological arguments given in the book. There really is an anti-intellectual on-campus movement to denounce 'materialistic science' in favor of something considerably more 'cold and unforgiving.' So watch it." (Special Thanks: The Mad Alchemist)

---

9. Bell Atlantic Shoots Themselves in the Foot (February 5, 1992) -- Newsbytes reports that Bell Atlantic admits having funded an advocacy group "Small Businesses for Advertising Choice" to oppose HR 3515, a bill regulating the RBOCs' entry into info services. Tennessee Democrat Jim Cooper, the sponsor, called it a "clumsy Astroturf campaign," meaning fake grass roots.

   Republican co-sponsor Dan Schaeffer was a target of a similar campaign by US West, in which telephone company employees were encouraged to call their representatives on company time to oppose the measure.

   The bill is HR 3515. To get a copy, call the House Documents Room at (202)225 3456 and ask for a copy. It's free (more accurately, you have already paid for it).

---

10. Computer Hackers Get Into Private Credit Records (Columbus Dispatch, February 24, 1992) -- DAYTON - Computer hackers obtained confidential credit reports of Midwest consumers from a credit reporting firm in Atlanta. Atlanta-based Equifax said a ring of 30 hackers in Dayton [Ohio] stole credit card numbers and bill-paying histories of the consumers by using an Equifax customer's password.

    Ronald J. Horst, security consultant for the company said the break-in apparently began in January. Police don't know if the password was stolen or if an employee of the client company cooperated with the hackers. Horst said the hackers were apparently doing it just for fun. No charges have been filed. Equifax will notify customers whose credit reports were taken.

---

11. Fingerprints And Connected Databases (Summary of an article by Stephen Schwartz, San Francisco Chronicle, February 22, 1992, Page A16) -- A fingerprint found in an unsolved 1984 murder of an 84-year-old woman was kept in the San Francisco police database all these years. Recently the San Francisco fingerprint database was linked with the Alameda County fingerprint database. The old print matched a new one taken in connection with a petty theft case, and so eight years later the police were able to solve the old case (burglary, arson, homicide). The two girls implicated were 12 and 15 at the time. (Special Thanks: Peter G. Neumann of RISKS)