within...

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.
Forwarding and Address Correction Requested

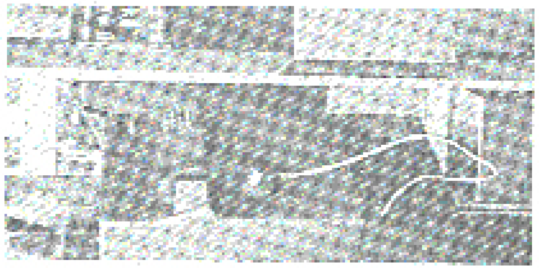
SECOND CLASS POSTAGE
Permit PAID at
East Setauket, N.Y.
11733
ISSN 0749-3851

2600

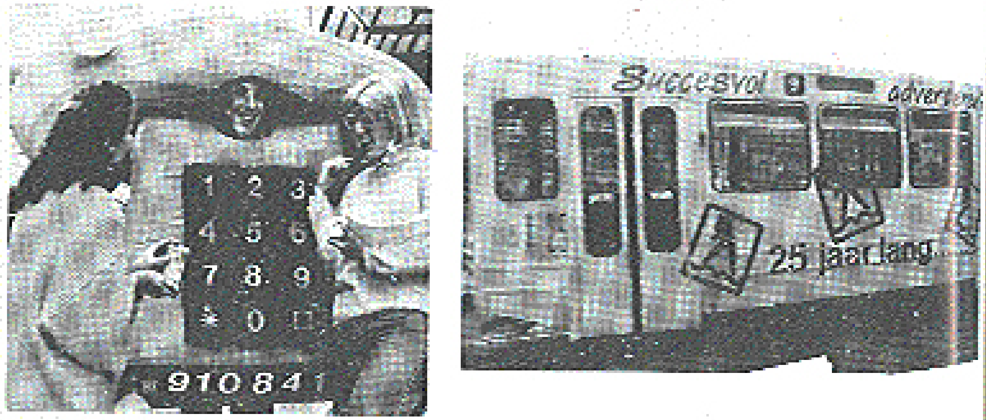
The Hacker Quarterly $4 *VOLUME SEVEN, NUMBER THREE*
AUTUMN, 1990

FRENCH COIN PHONES

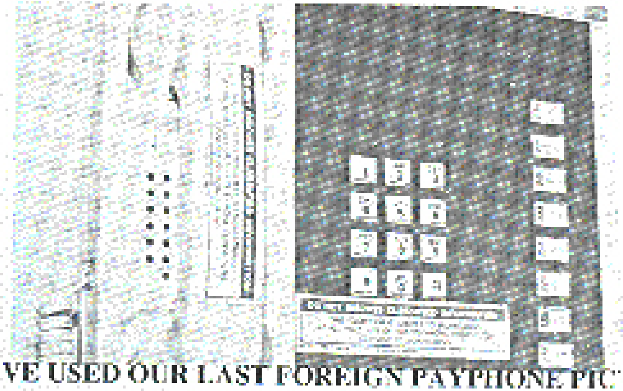
increasingly hard to find, but here's one in Paris (sideways)



STRANGE DAYS IN HOLLAND



AND MILITARY MADNESS



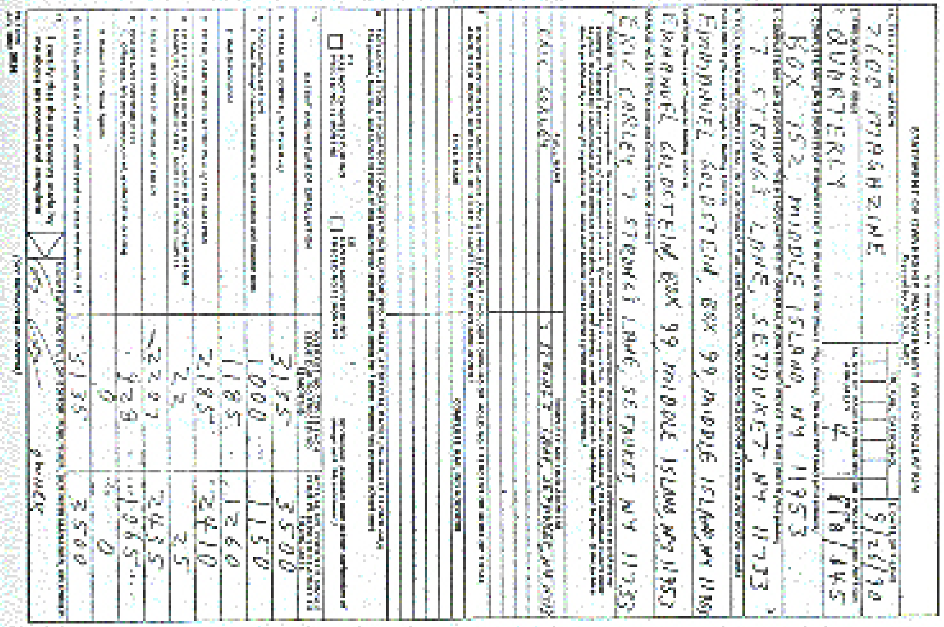
WE'VE USED OUR LAST FOREIGN PAYPHONE PICTURE! SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953. HURRY!!

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada --$18 individual, $45 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984, 1985, 1986, 1987, 1988, 1989
at $25 per year, $30 per year overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.
NETWORK ADDRESS: 2600@well.sf.ca.us.

2600 **Office Line: 516-751-2600,** *2600* **FAX Line: 516-751-2608**



STATEMENT OF OWNERSHIP, MANAGEMENT AND CIRCULATION

2600 MAGAZINE

9/21/90

QUARTERLY

4

$18/$45

BOX 752, MIDDLE ISLAND, NY 11953

7 STRONG'S LANE, SETAUKET, NY 11733

EMMANUEL GOLDSTEIN, BOX 99, MIDDLE ISLAND, NY 11953

EMMANUEL GOLDSTEIN, BOX 99, MIDDLE ISLAND, NY 11953

ERIC CORLEY, 7 STRONG'S LANE, SETAUKET NY 11733

ERIC CORLEY | 7 STRONG'S LANE, SETAUKET, NY 11733

A.	3125	3500
B. 1.	1000	1150
B. 2.	1185	1260
C.	2185	2410
D.	25	25
E.	2210	2435
F. 1.	928	1065
F. 2.	0	0
G.	3135	3500

CALLER ID: THE FACTS

by Jake "The Snake"

You've probably either heard of it, seen it in the media, or maybe you even own one of those little "buggers". There's been a lot of talk, fighting, and discussions in court over the Caller*ID box. Currently existing only in New Jersey, this device is basically a tracer. And, yes, it is legally available to the public.

In case you aren't aware of such a hacker's dream, let me fill you in on the details. The device itself is a small stand-alone unit, about 6"x4" weighing about 8-10 ounces, with a 32-character (5x8 pixels), 2-line display and a few buttons on the front. In size it resembles a simple desktop calculator from a couple of decades ago. It can run on a 9 volt or A/C adapter and has 2 RJ-11 jacks on the back, both identical, for attachment to wall and phone.

Caller*ID is offered along with many other "sister" services that I will explain later. Because of the AT&T divestiture a few years back, the local companies aren't authorized to sell the device itself but can only offer the service (at a cost of $21 for installation and a whopping $6.50 a month) to its customers. The box can be ordered from a few different distributors for anywhere between $60 and $300.

Let's say you purchased a Caller*ID (known as "ICLID" in the industry, which is an acronym for Incoming Call Line Identification Device) and hooked it up to your phone. This is how it would work: After your phone rings once, you'll see some information flash on the little LCD display. Models vary, but you'll definitely see the caller's phone number and current time and date. Most models store the numbers in memory for recall at any time. So, if you're not around to answer the call, you can be sure that anywhere from 14 to 70 numbers will be saved for your convenience. (It's great to be able to come home and see X number of messages on your answering machine and see X+4 callers on your ICLID. With a little matching up, you can figure out who didn't leave a message.)

Of course, there are drawbacks to our little "mirror box". What are the limitations to its tracing ability? First of all, it won't work without the local company providing the service. Only after the first ring does the information come storming down the line to be decoded by your little friend. (I have two lines in my house, and sometimes there's a bit of crosstalk between them. When the phone rings, if I listen carefully enough I can actually hear the coded ICLID information being sent.) Also, only areas that offer this service (and other "CLASS" Calling Services) to their customers will be traceable areas. But this area is growing.

If someone calls from out of state or from the boonies a message like "Out of Area" will be displayed instead of the number. That's the real bummer. But, all of the latest models of Caller*ID devices are area code compatible and show your area code where other NPAs will be in the near future. Many states have been slow to pick up the technology mainly because of political and legal reasons. Many privacy issues have been suggested and debated over, but we won't go into those here. As I understand it, New Jersey Bell contends that if a person has your number and calls you, you should have their number as well; when a connection is made, both ends should know who they're talking to. So, hopefully other states will get their asses in gear.

"With the public being offered these services, imagine what business customers, or even Sprint/MCI/AT&T are being offered?"

The option to block particular calls is being juggled around, too. Telephone companies are thinking of offering a service whereby the customer would dial a couple of digits before the 7-digit number and the receiver would get an "Out of Area", or similar, message on their ICLID display. This would definitely suck, unless you are the caller. But, this service is already available now thanks to a small loophole. I'll explain later.

New Jersey Bell started CLASS Calling Services around December of 1987. They were test marketed in Hudson County until December, 1988 and then began to spread. Other services include Priority*Call, Call*Block (a personal favorite), Repeat*Call, Select*Forward, Return*Call, Call*Trace, Tone*Block, and others. Many of these are based upon the instant tracing ability of CLASS.

Priority*Call will send you a distinctively different sounding ring when certain people call you. You program a "queue" of phone numbers that when called from, will sound different than the standard phone ringing.

Call*Block is lots of fun. Again, you can program a queue of people into your phone (really, the phone company's computer). When they call your line, they get a recorded message along the lines of, "I'm sorry. The party you have reached is not accepting calls from your telephone number." Nice and rude.

Call*Trace is a service that is available to everyone on a pay-per-trace basis. If you receive a prank, etc., you hang up, pick up, and immediately dial *57. A recording lets you know if the trace was good or bad, and you get charged $1.00 accordingly. Unfortunately you have to call the phone company to get the phone number. This service is for serious complaining and is meant for people who get pranked a lot and want to file charges.

All of the above features can be generally replaced with an ICLID. As a substitute for Call*Block I can simply not answer the phone if I don't want to speak to someone, since my ICLID lets me know who it is. Of course, that pre-recorded message adds a nice touch. Call*Trace is pretty much useless with ICLID unless you want to bring in the gestapo. But, then again, Call*Trace is open for anyone to use and isn't ordered monthly like the other services.

A woman from New Jersey Bell told me, though, some technical legalities regarding Call*Trace and Caller*ID: If someone pranks me, and I return their call (having read their number from my "mirror box") and prank them in return, they can *57 me and sue me for phone harassment. Even though I have their number on my ICLID, if I don't *57 him before I call him back, I get my ass kicked in. So, the moral of the story is that ICLID can't be used as evidence of a prank.

Select*Forward is used in connection with Call Forwarding and simply forwards only calls coming from numbers that you choose.

Repeat*Call doesn't have much to do with identifying the caller, but will simply redial a number until you get through, and then call you back when the line is free, allowing you to use the phone for other reasons. Sounds cool, eh? Now you can get through to any radio station you like, right? Wrong. It really isn't as great as it sounds. First of all, it only "redials" for 30 minutes. Also, it really doesn't dial the number, but only checks the computer to see if the line is free (and it checks only every 45 seconds). So, it is possible, and happens to me occasionally, that you pick up the phone when the computer calls you back to inform you that the line is free, and you find that it's busy again!

Return*Call is made for people who just make it out of the shower and to the phone a second after the caller hung up. Boo hoo. In a few keystrokes the call is returned, and the wet, naked person still has no idea what number (s)he returned.

And finally, Tone*Block turns off Call Waiting for individual calls. Pick up the phone, dial *70 and then the number. Voila! No interruptions. But let's say someone calls you. You cannot turn off your Call Waiting in this case, unless of course you also have 3-Way Calling. If you do, you may switch over to the other line and *70 yourself and you'll be fine for the call.

With instant tracing ability soon to sweep the nation, what's the nightmare? Well, basically this hacker's dream is not only for the hacker but for anyone who's got the cash and happens to live in a CLASS infested area. With the public being offered these services, imagine what business customers, or even Sprint/MCI/AT&T are being offered? When ICLID capabilities spread to more states, LCD displays will be showing more and more area codes. Eventually, long distance companies will integrate themselves, and for every telephone connection made, there will be two numbers involved and available to each

HACKERS' DREAM AND NIGHTMARE

end.

When I first got Caller*ID (the service was actually enabled on my line before I received the box) I wanted to learn as much about it as I could. So I played around with it and took it apart. The model that I have (which is relatively old, but there are more ancient ones, too) has a main board inside with some chips and components on it. By ribbon cable it is hooked to an LCD board with LSI chips. There are two buttons (Review and Delete) up front and a battery clip in the back. When the 30th call comes through, it scrolls old ones off to make way for the newest. (This has happened only once to me when I was away for an extended weekend.) What I like about my model is that it will store every call separately. On many models these days, if a call comes through more than once in a row (from the same number), the series of calls will appear under just one entry with a small "RPT" indicator for "repeated call". Personally, I like to know that a certain person called twice a minute for five minutes to get ahold of me, rather than just "Repeat". But that's a personal preference. The flip side is that the extra calls take up space in memory.

The main distributor for ICLIDs is Bell Atlantic Office Supplies (800-523-0552). They sell a few different models. Sears has also been allowed to sell ICLID's through AT&T (who has yet another company making them). Any Sears in New Jersey will sell you one for around $99.95. Radio Shack expects to be offering one soon. That's about it for being able to order them. But there are of course the manufacturers that build these things. Sometimes you can order them directly....

Currently, there are only four manufacturers around that I know of. In Irvine, CA is Sanbar, Inc. (800-373-4122 or 714-727-1911). Sanbar works jointly with another company called Resdel Communications, Inc. I was able to acquire some helpful information through Sanbar and their technical support. Colonial Data Technologies is located somewhere in the depths of Connecticut and makes most of the ICLIDs that Bell Atlantic and Sears/AT&T sell. They aren't too helpful when it comes to questions about Caller*ID, but their number is 800-622-5543. RDI in New Rochelle, NY recently created a smaller company, CIDCO, to produce ICLIDs, as the epytomology of the name might suggest. (I spoke with a fellow there named Bob Diamond. I was pretty embarrassed when, after a few conversations with him, I curiously asked what RDI stood for and found out it meant "Robert Diamond, Inc.") The other manufacturer is a major telephone equipment supplier. Northern Telecom has a massive set of complexes in the southern United States. They make a stand alone ICLID as well as the only living telephone with a Caller*ID display built in. It's known as the Maestro and can be ordered through Bell Atlantic. It's a simple thing with your basic features such as one-touch dialing, redial, hold, mute, etc.

One thing I aspired to do with my tracer was to try and interface it with my computer. If I could just get the information on the LCD to the serial or joystick port, I could write lots of fun programs. You're sleeping in bed and the phone rings. Unfortunately you're too tired to get up, turn on the light, and see who's calling (actually, CIDCO makes an ICLID with a backlit LCD display). But you left your computer running and within a few milliseconds it announces the person's name, and a Super VGA digitized picture flashes on the screen. Now you know who it is.

And the imagination can run wild with things to do with the computer integrated ICLID: auto-validating BBS's, database management, and so on. So, I called Sanbar (the manufacturer of mine) and talked to one of the head engineers. I asked him if there was any way to leech information from the unit. He said that piping it off the LCD was the best bet, but it might be easier to build a whole ICLID from scratch. After speaking with many people from many different companies, I finally worked on outputting from an LCD. Sanbar used a Sharp LM16255. From Sharp (who were very friendly and helpful) I received literature and specifications. Unfortunately I didn't get too far. Apparently the information is sent in nibbles to the LCD board in parallel format. One must know a bit about electronics and parallel port communications to wire it up.

But, fortunately, now there is at least one box available that sends the information via a serial port. (Ah! Such ease.) CIDCO is selling a "business model" that sends the information at 1200,N,8,1 through a serial port in the back. The price? $300. Too much for me. Other companies said they will have similar items, which I expect to be much cheaper.

As far as I know, there aren't many tricks or secrets about using your ICLID at home. When someone calls, either you get their number or you don't; I don't think any electrical modifications will be able to trace untraceable numbers. I hope I am wrong. When I first read the instruction "manual" (leaflet is more like it) I saw that Bell Atlantic had put a piece of tape over a part of the page. I guess they didn't have time to edit the paragraph out. It was in the section of the text showing all the different messages that my box could produce. (It can either show a) a phone number; b) "Out of Area"; or c) a junk number with a few question marks, indicating that there was static on the line or the phone was picked up during the information transmission after the first ring.) Looking at it through the light I saw that another possible message it could produce (and doesn't anymore) was "Private No.". I thought that was great! After speaking with New Jersey Bell, I found out that unlisted numbers are traced along with everything else! Pretty awesome; New Jersey Bell doesn't skimp.

"All of the latest models of Caller*ID devices are area-code compatible and show your area code where other NPAs will be in the near future."

If you have Call Waiting, you'll hear the tone, but unfortunately the ICLID won't trace the number. It needs that first ring to "wake it up", so the phone company doesn't bother to send any info. They tell you this in their brochures, but they don't tell you how you can still trace the number of the person who calls you (without going through *57, the main office, and a law enforcement agent). Here is how to do it: When you hear your Call Waiting, tell your friend that you'll call her back and hang up the phone. They will be disconnected and the phone will begin to ring for the person who originally clicked in. Call Waiting leaflets tell you this will happen, but no one tells you what happens next, after that first ring. Voila! Your ICLID will light up and will translate the data that was sent after the first ring. You've traced a call waiting!

As I mentioned earlier, the idea of a per-call block is being thrown around in courts and behind telephone company doors. Supposedly, soon you will be able to make "Private No." show up on your adversary's LCD display when you call. But, it's quite possible now. If you want to call someone and not have your number traced, all you need is a bit of plastic. No "boxes" or equipment. By going through your Sprint/MCI/AT&T Calling Card, the receiver will see an "Out of Area" message. That's what the phone company displays when the incoming call originates through a calling card. Voila! A blocked call. The only drawback is that small surcharge for using the card.

Recently, New Jersey Bell corrected a small computer bug that a bunch of friends and I were having a lot of fun with. When someone called my house collect, the number of their pay phone would show up, so I could reject the call and return it, paying nothing for the connection (assuming the pay phone was a local call). That didn't last for long, and now a collect call brings with it the anonymity of an "Out of Area" message. It was fun while it lasted.

The Network 2000 Saga Continues

EXECUTIVE [illegible]

Guarding Our Success: Protecting Against UNAUTHORIZED Accounts

By Jim Adams, Executive Vice President

We have the greatest network marketing program in America! Not only are we "the talk" of the network marketing industry, but our program has won high praise from top US Sprint executives who have recently awarded our reaching the one-millionth installed-customer mark in July. We're proud and excited about this outstanding achievement. NOTHING can keep us from being the biggest, the brightest and the best . . . nothing, that is, except unauthorized accounts.

I need your total commitment and help in eliminating this problem. As professionals and protectors of the integrity of our program, you need to make every effort to conquer this challenge NOW!

What Makes an UnAuthorized Account

An account is "unauthorized" when the customer claims not to have knowledge of requesting US Sprint long distance service, or claims not to have been informed regarding the details of receiving the service. A customer may be "unauthorized" because the customer:

- does not remember talking to IMR
- thought he or she was getting ONLY the FONCARDsm, when the IMR signed the customer for long distance service, too
- didn't know a fee would be charged to switch from another carrier
- was signed up for US Sprint service by a spouse, who didn't tell the "customer of record" about the change
- customer's signature was forged
- misinformed about 30 free minutes promotion

Correcting Mistakes

Needless to say, it is extremely rare that we find a problem with forged signatures (Signing a customer's name on a ballot is against the law, and grounds for immediate termination.) Most "unauthorized accounts" occur because the IMR was not clear about the details of the ballot.) When an IMR follows the Ron Windham Method of signing customers, there are no such misunderstandings. (Purchase and review the Wizard of Windham video, then practice the proper, professional way of getting customers for US Sprint.)

To eliminate "unauthorized accounts" in your organization, we recommend the following:

- Be certain the name on the ballot is the name the phone is currently listed under.
- Be certain the person signing up for the service understands:
  - ✓ They will receive their FONCARD in approximately 30 days.
  - ✓ They will ALSO have their long distance service changed over to US Sprint.
  - ✓ They will be charged a nominal fee by their local operating company to make the change. (Some IMRs appear to be operating under the misunderstanding that if a person has ALWAYS used AT&T, there is no charge for the customer's first change to another long distance carrier. THIS IS ABSOLUTELY FALSE. Over the past 18 months, I've never had a single person ever change their minds when I told them about the switch charge.)
- Explain the respective promotion in detail. If they select Dial-1 service, tell them that their 30 free minutes will appear as a credit in their third billing month. If they select Sprint Plus, inform them that they'll receive one month's free long distance (maximum $25) credited on their January 1990 bill.
- The ballot must be signed by *the customer in the presence of the IMR.*
- Give the new customer one of the new flyers immediately after they sign the US Sprint service request ballot. This great sales tool reinforces all the information you told the customer before they signed the ballot. (This flyer is a reinforcement of what you have said. DO NOT use the flyer *in place of* telling the customer this information.)
- Network 2000 has a fail-safe system for discovering unauthorized accounts. A toll-free number is supplied on the back of all US Sprint bills. Using this number, the customer notifies US Sprint that they did not authorize the service. US Sprint then notifies N2K of the situation. And because we have records of all IMRs and their customers, we are able to pinpoint the source of the problem.

What Happens if You Create an Unauthorized Account?

As you know, we are now tracking unauthorized accounts. And we are requiring IMRs who incur these accounts to make an explanation. When unauthorized accounts are found to be the result of IMR neglect or misconduct, disciplinary action (which could include suspension or termination as an IMR) is mandatory.

Again, I congratulate your professionalism. Unauthorized accounts are a threat to our program; we must all work to guarantee they do not occur. Which is why again I say that as protectors of the integrity of our fine program, you *make the difference!*

We've printed stories in the past about Network 2000 signing up people for Sprint's long distance service without the customer's consent. This page from a Network 2000 newsletter shows that they are very aware of the problem.

Nice Telephone Company

CABLE & WIRELESS
COMMUNICATIONS, INC.
1919 Gallows Road
Vienna, Virginia 22182
(703) 790-5300

October 30, 1990

Dear Long Island Customer:

We deeply regret any inconvenience caused when your long distance service was interrupted on Monday, October 29. Although we cannot replace the calling time your business lost that day, we want to compensate you for your trouble. Therefore:

> **On Monday, November 5, 1990, between the hours of 9:00 a.m. and 12:00 noon, 100% of your long distance calls will be ABSOLUTELY FREE. That includes instate, interstate, international, 800 and travel calls -- everything!**

Again, we apologize for your inconvenience and appreciate your patience. Thank you for being a valued Cable & Wireless customer.

Sincerely,

Charles J. Gibney
Senior Vice President
for Marketing and Sales

Almost nobody heard about this incident. We weren't even aware of a service disruption! Of course, we didn't get this letter until the 6th, but it's the thought that counts, right?

Nasty Telephone Company

AT&T

Reference: [redacted]

Dear [redacted],

Thank you for applying for the AT&T Universal Card.

We regret that we are unable to grant your request at this time because:

```
     YOUR CREDIT HISTORY INCLUDES INSUFFICIENT PAYMENT HISTORY
     YOUR CREDIT HISTORY INCLUDES SLOW AND/OR PAST DUE PAYMENTS
     YOUR APPLICATION INFORMATION DOES NOT MEET OUR PROGRAM REQUIREMENTS
```

This information was provided by:

```
TRW CREDIT DATA
[illegible] 12 MILE RD STE 335
FARMINGTON HILLS   MI          [illegible]
313-[illegible]
```

If you feel the information is incorrect, we urge you to contact the credit bureau to resolve the issue, and reapply for the AT&T Universal Card.

Of course, if you are an AT&T Calling Card holder, you may continue to use your AT&T Calling Card. Please be assured that AT&T values your continued business.

If you have any questions, please call me toll-free at 1 (800) [illegible] between the hours of 8:30 a.m. and 11:00 p.m. (ET), Monday through Friday.

Sincerely,

[illegible]
Credit Relationships

In other words, we value your business, but no way are we going to trust you.

an interview with dorothy denning

by Dr. Williams

Recently, I had the pleasure of posing questions to Dr. Dorothy Denning. Dr. Denning has been visible lately to the hacker community.

She participated with Sheldon Zenner in the defense of Craig Neidorf, and has written a paper, "Concerning Hackers Who Break Into Computer Systems". The paper was presented at a conference in Washington D.C., where she also moderated a panel "Hackers: Who are They?", in which Emmanuel Goldstein, Craig Neidorf, Sheldon Zenner, Frank Drake, Katie Hafner, and Gordon Meyer participated.

Dr. Dorothy Denning is well known in the computer security community as author of "Cryptography and Data Security" and numerous research papers. She is past President of the International Association for Cryptologic Research and works in Palo Alto.

This interview was conducted via e-mail over a two-month period.

Many members of the Computer Underground community believe there is a witch hunt afoot against hackers. Buck BloomBecker relates in his book, "Spectacular Computer Crimes" how Kevin Mitnick was harshly prosecuted by officials out to "get the little shit." Operation Sun Devil utilized the efforts of over 150 agents, seizing equipment in 26 locations, but making only 9 arrests, 7 of these computer related.

Finally, even though the prosecutor in Craig Neidorf's trail is to be commended for dropping all charges instead of handing the matter over to the jury, the fact the trial was started and later dropped leads one to believe they too were caught up in the witch hunt mentality before seeing the light. More examples exist. Do you think hackers are being persecuted by law enforcement fueled on by fear and ignorance, or are Computer Underground members not looking past their own bias to accurately judge the current state of affairs?

Let me begin by saying that I am not speaking on behalf of my company.

When I first heard the "witch hunt" analogy, it seemed to make sense.

Most computer crime is committed by insiders, and it seemed like law enforcement was over-reacting to the actual threat posed by hackers.

But as I've dug into some of the cases further and talked with people in law enforcement and industry, I've seen that some of the reports floating around in the computer underground were exaggerated, misleading, and failed to tell the whole story. Some companies have suffered large financial losses because of hackers.

So, the bottom line is that I do not agree that there is a witch hunt, but I can see how people could see it that way. It is true there are more serious problems in this country than that caused by hackers, but this does not mean the damages caused by hackers should be ignored.

Craig Neidorf's trial raises a plethora of questions. At the heart of the issue is why was the trial ever started in the first place.

Even to the casual observer familiar with Phrack, both sets of indictments appeared to be based more on inference than fact. The prosecutor's strongest card was showing the LOD/H was a band of rogue hackers and that Phrack and Craig Neidorf were associated with them, which implies weak evidence on the prosecutor's part. One cannot help but get the feeling Bell South and the Secret Service were pushing hard for this trial - one could suggest pushing past the point of seeking justice. Bell South was embarrassed by the publication of its E911 text document in Phrack and had hidden damaging evidence from the prosecutor. The Secret Service, after expending the efforts of over 150 agents in Operation Sun Devil and claiming a national crackdown on hackers, but making only nine arrests, seemed to be grasping at straws and interested in saving a little face. It is no secret many disapproved of Phrack's content: bomb recipes, password crackers, hacking tips, lock picking suggestions, etc. The philosophizing could go on and on as more points are considered. Why did you think Craig Neidorf was really prosecuted?

I believe that the government prosecuted Neidorf because they thought he had broken the law. I believe that they accepted, perhaps without questioning, Bell South's claim that the E911 document was highly sensitive and proprietary and that a hacker could use it to disrupt 911 service.

What was your motivation to be involved in Craig Neidorf's trail?

I believed he had not broken the law and that I could help with his defense. I was also concerned that a wrongful conviction — a distinct possibility in a highly technical trial — could have a negative impact on freedom of the press for electronic publications.

Many people feel the government was looking for the first opportunity to send a message that Phrack was not an acceptable publication. Do you speculate this is why the government accepted Bell South's claims without questioning?

While it may be true that the government disapproved of Phrack, I know of no evidence that suggests this was a reason for prosecuting.

I speculate that the government just never considered the possibility that the information they got from Bell South could be wrong and not hold up in court. I hope that in the future they will consult with disinterested experts before deciding whether to pursue an indictment.

Many articles in CU Digest and elsewhere have been critical of current laws governing hackers, viruses, computer usage, information concerning hacking and computer weaknesses, and fraud associated with computers on several grounds. Some laws have been shaped and enacted in crisis more by fear and misunderstanding than truth and good sense. Other laws dangerously erode our civil rights, fail to assign responsibility to computer owners to protect data, dish out harsher penalties to computer crimes over comparative crimes, do not give electronic media the same rights and privileges of printed media, have been motivated more by politics than protections, and in short, are just plain stupid, archaic, and frightening.

What is your opinion of the general worthiness of current laws governing hackers, viruses, computer usage, information concerning hacking and computer weaknesses, and fraud associated with computers?

I am not aware of any computer crime laws that erode civil rights or fail to give electronic media the same rights and privileges of printed media. Also, there are none that I assess as stupid, archaic, or frightening. While many laws may be initiated by a crisis, they generally undergo extensive review, sometimes over a period of several years, before they are adopted. Overall, I'd say the laws are pretty good. As deficiencies are discovered, they get amended and new laws added.

Current laws may provide a means of assigning responsibility to computer owners to protect data. I expect that an individual or company could sue an owner for failing to protect information about them, or failing to provide a promised service because negligent security practices allowed an unauthorized break-in. Nevertheless, I believe it is worthwhile to consider adopting a law where unauthorized entry into a system is at most a misdemeanor if certain standards are not followed and the damage to information on the system is not high. The difficulty is that it may be very hard to set appropriate standards and to determine whether an organization has adhered to them. Currently, it takes several years to evaluate a product according to the Department of Defense Trusted Computer System Evaluation Criteria.

For the most part, the penalties given to persons convicted of computer crimes have seemed reasonable. Although it can be frightening to see someone such as Neidorf facing 65 years in prison, it is fantasy to believe that a judge would assign anything even close to that. Most judges are fair and reasonable; this is why they are trusted with that position. If they assign a penalty that is unfair, public outrage will force them to reduce it. Still, it would be worthwhile to consider establishing a range of offenses with different penalties.

Information concerning hacking and computer fraud is sparse and often misleading. This is a consequence of the fact that the actual evidence in a case cannot be fully disclosed until the case comes to trial.

In addition, companies do not talk about hacker incidents since doing so is perceived to be harmful to business.

Information about computer weaknesses is widely disseminated through conferences, newsletters, professional journals, computer security courses, the CERT, and human networks.

Your paper, "Concerning Hackers Who Break into Computer Systems," states one of the motivations behind hackers is a belief in the free flow of information. Free flow of information has helped propel us to our current heights of technology. Now, hackers point out the disturbing trend of treating information as property instead of the particular way information is expressed. Hackers feel restriction of information will deter learning and hurt the evolutionary process of technology. When information is kept secret behind computer doors, the

dorothy denning interview

result is bad for all of us. As the way Richard Stallman explains the statement in your paper, "I believe that all generally useful information should be free", do you agree with that point of view?

This is a tough issue on which I have more questions than answers.

On the surface it sounds compelling, at least for certain types of information, and I have always tried to operate from that principle myself by making my research results public. Stallman's arguments against software patents and user interface copyrights are especially convincing. The topic is definitely worth exploring and discussing.

But in any case, I believe it is wrong to use this principle to justify going into a computer system and downloading information to which you are not authorized, or to disseminate information obtained thusly.

One result of secured computers is secured information. What would be your reaction if the results of your research and work were applied to restrict the flow of information in a manner you morally disagree with? Does the effect of computer security on the flow of information ever concerned you?

Computer security per se does not restrict the flow of information. People do. If I want to restrict the flow of some information, I always have the option of not storing it on a computer at all or storing it on an isolated system. Indeed, these methods of handling sensitive data have been a common practice precisely because adequate security mechanisms were not available. The problem with these practices is that they also make it more difficult for people who need to have access to the information to do their work effectively. Computer security gives people the capability to computerize sensitive information and integrate it with other information more easily. This can be a big productivity boost. It makes controlled sharing and distribution of information easier. If I'm on a network that provides a secure cryptographic facility, then I can use the net to send you a highly confidential report without worrying about someone else reading it. By providing mechanisms for controlled sharing, computer security does not restrict the flow of information so much as give you assurance that the information will be disseminated according to your wishes.

Even then, the assurances are weak unless you use mandatory policies for information flow, that is, policies based on classification and clearances and a strict rule forbidding the transfer of information from one security level to a lower one. But most organizations other than the military find mandatory policies too restrictive, and so adopt discretionary ones. With a discretionary policy, it is very hard to control what happens to information once you give anyone access to it. You have to trust that the other people will respect your wishes. Fortunately, most people do, so the lack of assurance may not be a practical problem.

Since I don't want to avoid your ethical question, let me try to outline a scenario that I think gets at it. Suppose that I know of some information that in my assessment will result in harm if it is not freely distributed, but that the person who produced the information is not letting it out. Suppose further that I know the information is stored on some system with a security mechanism that I designed, and that without that mechanism, someone could get access to the information. How would I react? I have never been in a situation like this, so it's hard for me to say for sure what I'd do. I expect I'd go to the person with the information to find out why he or she does not want to give the information out. My own view of the world is extremely small, so there may be some good reasons that I have not thought of. If I am not satisfied with the answer and I know what the information is and not just what it is about, I might consider disseminating the information myself. But, I would have to have very strong reasons for doing this, since the consequences to me or to others could be serious. Another action I might take would be to try to exert public pressure, e.g., by going to the media and reporting that so-and-so is hoarding this information. I might do nothing on the grounds that if the person who produced it had not been there, we would be no better off.

It's been said computer crime costs everybody. However, this statement is often said in glib without much underlying thought. Can you explain if and how computer crime effects everyone in two different examples?

Situation 1: Ten different department stores operate in one region. One store, Store A, is the victim of a computer crime costing a modest amount of its profits for the year. How then is everybody effected, customers and non-customers? Nothing has happened to the nine other stores, so life is exactly the same for all their customers. Raising prices to make up for the loss by Store A would backlash. In a competitive environment, customers of the victimized store would simply buy the same items priced less at the nine other stores, compounding Store A's losses further. It could be argued the lost money could have been used to pay bigger dividends to stockholders, be used for charitable contributions, increased customer services, etc. In any scenario, counter arguments exist. Only a limited amount of people feel the loss, such as the stockholders, not everybody. If the lost money were to be spread around in a manner that truly touched everyone, the amount per person would be so minute to make its effect wholly ignorable. Finally, there are the doubts that if Store A had never lost the money, it would have been used in a manner that effects everyone in the first place.

Situation 2: A company earns $1.5 million dollars profit one year.

At the end of the year, a hacker breaks into their computers. The total cost to clean up his damage is 0.1 million dollars. How is everybody effected? It is not likely the company will specifically raise its prices next year to make up the lost 0.1 million. Instead, it will probably settle for $1.4 million dollars profit and a tax write off.

Again, the arguments could place the lost money being used for employee benefits, additional R&D efforts, etc. This moves back to the counter arguments of the last paragraph and leaves the question, "How is everybody effected?" Clearly, computer crime is wrong. These arguments are not made as an attempt to justify or lessen the effects of computer crime, but made in hopes of clarifying hard points.

In both situations, you identified the direct financial costs to the companies involved resulting from the crime itself, and then analyzed how these costs are transferred to individuals. In both cases, the costs that reach most individuals seem negligible — unless you're the employee that lost his or her job because of the reduced revenue.

However, the financial costs to the companies can be even greater if publicity about the crime leads to loss of credibility.

When people say that computer crime costs everybody, they are usually referring to indirect costs. The indirect costs include increased tax dollars for law enforcement to fight computer crime, for research and development in computer security, and for government funded organizations such as the National Computer Security Center and the Computer Emergency Response Team. Indirect costs also include expenditures by vendors to develop secure products and by companies for security personnel, products, and training to protect their assets and operations. These costs, which may rise in response to increases in criminal activity, are passed on to customers. In your first situation, all ten department stores may feel compelled to beef up their security, and then raise their prices to absorb the costs.

Similarly, in your second situation, many companies operating on tighter profit margins may respond to a concern for suffering a similar loss by making security enhancements and raising prices.

I should point out that I do not view the above costs as bad, in the same way that I do not view the cost of airport security as bad. As a result of the latter, I can trust that the airplane I board is highly unlikely to be hijacked or blow up from a bomb. Similarly, if I have a secure system, I can trust it to preserve the secrecy and integrity of valuable information assets, and I can be confident that its operation will not be sabotaged.

But, some people say that security places a burden on users. Perhaps an analogy with the Tylenol scare is appropriate. As a result of one incident, it is now a major project just to open a bottle of vitamins!

A consequence of computer crime may be computer surveillance. Because of the widespread concern about break-ins and other forms of computer crime, computer security specialists are developing intrusion detection systems that will monitor systems for break-ins and other forms of abuse. If such systems are not carefully thought out and used, they could result in loss of privacy and degradation of trust in the workplace.

How has the proliferation of workstations changed the needs of computer security?

When workstations were first introduced, many people claimed they would solve the computer security problems of time sharing systems, because users and data would be isolated. In practice, they have introduced at least as many problems as they have solved, because nobody wants an isolated

an interview with dorothy denning

workstation. One challenge is to protect a workstation from attack by untrusted users and software running on other systems that are connected to the workstation. Sun, for example, recently announced a patch for a security hole in SunView that allowed any remote system to read selected files from a workstation running SunView. Authentication of users, workstations, and software is becoming an increasingly important issue in networked environments in order to make sure that a remote request for service comes from the person or workstation claimed, and to make sure that programs such as login have not been replaced by Trojan horses or contaminated with viruses. A problem that arises with a workstation placed in a public place is how you prevent someone from rebooting the workstation, gaining root privileges, and then causing trouble on that workstation or other systems on the network.

Computer security scientists have developed good computer security procedures, but their record for simply preaching the practice of these developed procedures is less impressive. Today, many computer managers still fail to exercise basic computer security defenses. Can computer security scientists be faulted for failing to impale good security precautions into computer operators, or is that pointing the finger at the wrong person? Everybody plays a part is computer security, but who is most responsible: the user to use basic common sense, the operator to use tools already available, the vendor to develop secure OS's, or scientists to make computers more secure?

Everybody shares the responsibility. Individuals and organizations should look for ways to take greater responsibility rather than for excuses to assign it to others.

Some people in the security industry and system administrators I have had the pleasure of talking to essentially consider hackers to be gum on the bottom of your shoe: They usually get in only when security is weak, are more annoying than dangerous, lack the reason to cause harm but have the ignorance to, and just have the potential to cause an unpleasant mess. While this certainly isn't a glamorous analogy for hackers, would you consider it essentially correct?

It is a nice analogy, but it fails to tell the whole story. Some organizations report considerable losses from hacking and phreaking incidents. To them, hackers are a serious menace.

Do you think BBS's, by their nature, should be regulated as common carriers or as primary publications? Some have suggested regulating BBS's similar to Ham radios and Ham operators. Do you think this suggestion has merit?

Computer bulletin boards have been referred to metaphorically as electronic meeting places where assembly of people is not constrained by time or distance. Public boards are also a form of electronic publication. It would seem, therefore, that they are protected by the Constitution in the same way that public meeting places and non-electronic publications such as newspapers are protected. This, of course, does not necessarily mean they should be free of all controls, just as public meetings are not entirely free of control.

In comparison to the severity of other crimes, hacking still makes relatively big headlines. Hacking's novelty has worn off, so why do you suppose it still continues to captures the press's fancy?

Recent articles have focused more on the constitutional issues raised by the Neidorf and Steve Jackson Games cases.

Your latest area of research concerns hackers. What is your personal motivation or interest to study hackers? Can you give us your answer to the question of your October '90 Washington D.C. conference, "Hackers: Who are They?"

Curiosity and a concern about the growing number of young people committing computer crimes that adversely affect the companies owning the systems they attack. I'm still learning who hackers are. They're all different, of course, while sharing a discourse that is revealed in places like 2600.

The few I have talked with extensively have been helpful, candid, passionately interested in technology and learning, and ethically conscious and concerned about unethical behavior and the free flow of information in organizations and society. I have enjoyed talking with them. But I would not want to say all hackers are like the ones I've talked with. Many hackers may be unaware or unconcerned about the adverse consequences of their actions on others.

Hackers can be notorious for bragging and showing off at the mouth, in verbal and in text. From your studies, would you say this is one of the greatest reasons leading to their capture and demise? If the characteristics of hackers are homogeneous enough to generalize, what is the typical life cycle of a hacker? Discovery and interest in computers at adolescence, hacker status by high school, in college and in trouble by 21, retired by 22?

Hackers are caught because they perform an act that someone in the company affected by the act assesses is serious enough to investigate, and because there is enough evidence to trace the act to the hacker. Cliff Stoll's book gives a good account of one such case. I haven't talked to enough hackers to know the typical life cycle.

Your husband, Peter Denning, is also a computer security scientist. Do your shared careers ever present interesting situations at home, i.e. stimulating dinner topics, computer religion debates, elaboration of projects, etc.?

Peter is a computer scientist, but security is just one of many areas he's interested in. He is by far my biggest supporter and biggest critic. I mean the latter in a positive way. He goes over all of my papers and offers comments and editorial suggestions. We have lots of interesting discussions, which often lead to new ideas and projects.

For example, the topic of my most recent paper on the Data Encryption Standard came up in a conversation. We never have computer religion debates. I showed Peter my response to this question, and the following dialog took place:

P: When you've been together for 18 years, you don't have many disagreements. You can't even tell where the ideas originate.

D: It has nothing to do with 18 years. We've never disagreed much on computer issues.

P: I completely disagree!

It has been predicted that passive eavesdropping will become the hacking of the 90's. This seems credible as prices in surveillance equipment have dropped over the years. How do you think hacking will change during the next decade?

Well, I don't have any special talents with a crystal ball, but it seems that if the motivation behind hacking is learning about and exploring systems, then I would not expect to see many hackers engaged in passing eavesdropping. Or, is the real motivation to have fun with technology in an illicit way? I expect that there will always be some hackers who try to break through security mechanisms, despite the risks and penalties of getting caught.

Many systems will be practically impenetrable because of improvements in security, but there will be always be systems that are easy to penetrate. As computer security tightens, the attacks may get more sophisticated.

I speculate that there will be more attacks on computers for purposes of espionage, sabotage, or fraud. These attacks will be performed by organized crime, terrorist groups, spies, and individuals out to make a profit illegally. I have heard that organized crime is already trying to enlist hackers, and some hackers may become criminals this way.

You stated your original intent for accepting the Sir Francis Drake interview in W.O.R.M. was the hope of teaching hackers something. Unfortunately, the interview did not move into that direction. What was it you wanted to tell hackers?

The hope was that I might say something so elegant and convincing that it would have the effect of discouraging hackers from breaking into systems. Which reminds me of a wonderful story by Raymond Smullyan in "This Book Needs No Title." Called "Another Sad Story," he describes a man who being overcome with mystical insight, wrote voluminously. When he finished writing, he read his manuscripts over with great pride and joy. Then one day, several years later, he reread his manuscript and could not understand a word of it.

Dorothy Denning can be reached on the Internet at "denning@src.dec.com".

NEW REVELATIONS FROM BELLSOUTH

by Emmanuel Goldstein

2600 has obtained internal documents detailing BellSouth's future plans for monitoring telephone lines. Their desire is to develop a system more flexible and powerful than that currently allowed by the Dialed Number Recorder (DNR). Its purpose, according to one of the documents, is "to assist our security personal [sic] in identifying intrusions across the telephone network."

What BellSouth is developing here is truly frightening — the ability to spy on any kind of conversation (voice, data, fax) literally at the touch of a button. Add to this the fact that everything obtained will be stored on computers and the potential abuses of this technology shine far brighter than any benefits.

An Overview

The system is to be made up of two separate components: a control unit and a remote unit (used for the actual monitoring). Both of these would be capable of allowing multiple units.

According to BellSouth: "The control unit will be located in a secure area, under the supervision and control of BellSouth Security personnel. This device is to be used to program and control the remote unit(s), gather data, and produce statistics. The telephone network and modem technology is to be the primary means of communications between the remote and control units."

The company is planning to purchase one control unit and four remote units. Each control unit, however, will be able to handle at least 50 remote units. Their long range plans are described as being able to cover up to six metropolitan areas.

Among the features BellSouth described as mandatory was a way of indicating the presence of fax or data communications occurring on the line and presumably capturing them. As for voice communications, the remote unit will be able to "record all analog signals occurring on the targeted number" upon receiving a command from the control unit.

Communications between the two devices are to be encrypted. The monitoring device (remote unit) will be capable of holding the data it captures until the control unit tells it to transfer the information. Doing this will not prevent it from capturing more data at the same time.

Among the information to be exchanged between the two units is an identification code indicating the target number. This code would be translated within the control unit. The company seems especially concerned at not having the actual phone number revealed in any communications. Another piece of data would be a "call sequence number" designed to keep track of the number of communications between the two devices.

Other information includes standard DNR-type data: time the phone was picked up, what numbers were dialed (rotary or pulse), time the phone was hung up. Each single call will be capable of holding 300 digits and dialing *within* a call is also to be time-stamped.

The information on the monitoring device would be held in Random Access Memory (RAM). Also in RAM will be "characterization data" such as the telephone number of the control unit and the alphanumeric unit identification code mentioned above. BellSouth estimates that 64K of RAM will be enough to store data on twenty dialing sessions or 24 hours worth of calls.

Listening In

All of these monitoring devices will be capable of listening to everything on the line, which makes them radically different from DNR's. "When activated," a BellSouth document reads, "all signals, voice, data, and fax, detected on the target number line are to be passed to the control unit using the communications data link between the remote and control location. The mode of transmission is to be simplex, towards the control unit. The activation of this capability is to be under control of the control unit and will be downloaded to the remote unit at time of activation." The control unit will be able to connect a call from the remote unit directly to a tape recorder. The control unit will also be able to tell the monitoring device to only listen when the phone is off hook or to listen at all times.

The monitoring device is supposed to be able to call the control unit when certain conditions are met, such as the memory being full or at a predetermined time of day. It can also call whenever a call is made from or to the targeted number or whenever a certain *type* of call is initiated, i.e., fax or data. Theoretically, this could also mean calls to a certain area code or to a specific number would enable the remote unit to call home.

PRIVATE
The information contained herein should not be disclosed to unauthorized persons. It is meant solely for use by authorized BellSouth Employees.

Security Features

The two units will be communicating over the regular telephone network via modem, although there will be the ability to communicate in a "private line environment". To prevent unauthorized access, the units will be silent when called. They will only become activated when the right password is entered at the right protocol by the calling device. BellSouth also suggests having "an artificial audible ring" emanate from both of the devices. Communications protocols under consideration appear to be X-modem and AX.25 with a preference for the latter.

Data received by the control unit will require a multi-tasking computer. Operating systems such as OS-2, Unix, and Xenix are being considered. In addition to storing data on a hard disk, tape backups are also likely. Backup control units are also being planned, in case one fails.

As far as physical makeup, each of the remote units, according to one of the documents, will be less than eight inches high, ten inches long, and three inches deep. They will also be capable of running on 60 hertz with internal batteries that will last at least two hours. Both the remote and control units will be capable of future expansion.

The Potentials

Everything seems to indicate that this system is designed for sticking a remote monitoring device in a location *anywhere* between the central office and the target telephone.

You may have already asked yourself a very good question. Why would BellSouth come up with such a system when they could just operate the whole thing out of a central office? Why bother with all of this communication between two units, synchronization, passwords, another phone line, etc.?

Although it was never stated, it appears that this system will be ideal for any agency interested in monitoring certain individuals. Who says the control units have to be located within the phone company at all? It could be anywhere. This kind of monitoring system can operate quite well without the phone company even getting involved.

Under the guise of protecting its system against intrusion, BellSouth is creating a monster. And it now appears that other phone companies around the nation are involved in this as well. The one thing needed for such projects to succeed is continued consumer ignorance.

more things you really shouldn't know

The following technical synopsis was prepared by the Fraud Division of the U.S. Secret Service and obtained by 2600. While it is stated that this noncopyrighted information is not intended for the news media, it should be noted that it has been rather widely distributed within the industry. We feel our readers and the general public have the right to know the facts in this case, or at least the facts according to the Secret Service. For those that haven't seen it in the papers, the phone company referred to here is GTE.

On February 4, 1989, U.S. Secret Service agents arrested four individuals in Los Angeles and one in Lincoln, Nebraska, for producing counterfeited Automated Teller Machine (ATM) debit cards and for possession of access device-making equipment. When the defendants in Los Angeles were arrested they were in the process of encoding the counterfeit ATM cards with stolen bank account information.

The group was planning to travel to a number of cities throughout the United States to make cash withdrawals from ATMs linked to a specific nationwide ATM network. They made plans to travel in teams to different geographic areas of the country and to use disguises to defeat ATM surveillance cameras, while using each card to its daily maximum for three to five days.

The counterfeit cards were constructed of posterboard cut to the appropriate size and affixed with common magnetic tape. The tape was encoded with stolen cardholder account data on Track 2 for use in ATMs.

Seized concurrent with the arrests were a computer, an encoding device, and thousands of counterfeit ATM cards.

The defendants intended to execute the scheme over a five day period during February, 1989. "Test" cards had been successfully used in at least three cities, which netted the defendants about $5,000.

This case constitutes the first known attack of this magnitude on a major nationwide ATM network.

Bank officials interviewed after the arrests confirmed that the account numbers used in this case would have given the defendants access to the checking accounts, savings accounts, and any lines-of-credit available to the legitimate cardholders. An audit of those accounts revealed this scheme could have netted the defendants as much as five and one-half million dollars had all gone according to plan and had the scheme gone undetected.

One industry expert from outside the bank speculated that it is plausible someone could, using this scheme or one similar to it, access accounts and steal as much as $100 million if carried to the extreme and extended over a 30 day period with careful execution.

In the city where this conspiracy began, several national and regional ATM networks share a single telecommunications carrier which routes transactions between ATMs and banks.

In addition, the telecommunications company, through a subsidiary, maintains a number of ATMs in a proprietary network which they make available on a contractual basis for other networks to use as ATM outlets for their respective cards. Thus, the role of the subsidiary company is similar to that of any bank on the telecommunications network.

The mastermind of this scheme was a computer programmer employed by a well-established software company specializing in the design and implementation of ATM network software. His company was contracted by the telecommunications company to update and expand the existing proprietary network.

The primary defendant's function as a programmer was to implement software which drove ATMs and Point-of-Sale (POS) terminals on the proprietary network in order to make information compatible with, and therefore acceptable to, the main electronic switch maintained for all of the participating networks on the communications system. His position required him to have access to most of the technical data pertaining to software for both the proprietary ATM network as well as the main communications system on which all of the networks were mixed.

In keeping with established industry standards, the telephone carrier subsidiary in this case encrypted the Personal Identification Numbers (PINs) used in conjunction with ATM cards. This was done prior to transmitting data from the ATM across the proprietary system to the electronic switch where the transaction would be routed to the appropriate bank.

The system targeted in this case is typical of ATM networks found throughout the United States. When a cardholder accesses his account through use of a debit (or credit) card at an ATM machine, the customer is asked to key in his or her Personal Identification Number (PIN). The PIN is encrypted using the universal Data Encryption Standard (DES) method, employing an encryption key known only to the owners of the proprietary system to which that ATM belongs. The account number and other Track 2 data from the ATM card, encrypted PIN, and information about the requested transaction are then transmitted electronically to a switch maintained by a designated communications carrier.

At the electronic switch, messages from several proprietary systems are received and decrypted, using the same DES key as was used to encrypt the data. At that point the information is sorted by the destination bank and encrypted with the proper DES key provided by the destination bank. The transaction is then transmitted across the main communications line to the appropriate bank.

(Theoretically, upon receipt at the bank, the information is once again decrypted using the key supplied to the communications network. However, in practice this step may not actually take place as the recipient bank may elect to accept the encrypted version of the PIN and process it in its encrypted form.)

Upon receipt at the bank, the account is queried and a determination is made relative to authorization or denial of the requested transaction. The flow of information is reversed upon return of a message from the bank to the originating ATM.

To illustrate, if Bank "A" issues ATM cards and maintains their own ATMs at various locations, they are running a proprietary system. A communications carrier must be employed to tie the system together but since there are no other participating banks on the system, the sorting process at the previously described electronic switch need not take place — all transactions are directly between the ATMs and the bank. Even on a closed system such as this, the industry encourages the use of PIN encryption. Furthermore, DES is the preferred standard when PIN encryption is employed.

On the other hand, if Bank "A" elected to enjoy reciprocity with Banks "B" and "C", permitting transactions at all three banks' ATMs, then an electronic switch would be installed to sort and route transactions between all of the ATMs and Banks "A", "B", and "C".

Transactions destined for Banks "B" or "C" from ATMs owned and operated by Bank "A" would still be considered to be on the Bank "A" proprietary system until they reached the electronic switch, where they would be mixed and sorted by the destination bank. At that point, the proprietary ATM networks from Banks "A", "B", and "C" combine to share a common communications carrier, but the networks remain independent and do not share encryption keys. The function of the electronic communications switch is to sort the transactions, determine which encryption key to use and establish how to route the information to the destination.

The system abused in the case in which these arrests were made was similar to that previously described, with the communications carrier subsidiary functioning in the role of Bank "A".

Specifically, the subsidiary owned a network of ATMs and, through a contractual arrangement, accepted debit/credit cards issued by various banks and honored by other networks. When a transaction was requested, the information was handled on the proprietary network until it reached a communications switch where it was decrypted then encrypted with the proper key for the destination bank, and fed into the main communications line used by all of the proprietary systems cooperating in this enterprise.

As a part of their routine business practice, the subsidiary recorded all transactions on the proprietary network before those transactions reached the electronic switch. The intended purpose was to create a transaction log from which all activities could be reconstructed should a system or other failure occur. The PINs remained encrypted in this recording process.

Either while performing his job, or merely by knowing where to look based on his intimate knowledge of the system, the scheme's mastermind discovered that the key used to encrypt PINs on the proprietary network was a default key, as opposed to a proprietary key selected by network officials. (A default key in an ATM machine encryption device is analogous to a common computer password installed by a mainframe computer manufacturer. Its intended purpose is for testing during the installation phase and it is expected that the default password will be removed once the system is installed and accepted by the buyer).

Upon making this accidental discovery, the programmer realized the value of this information and was able to refer to various software manuals and textbook literature to decipher the key.

The programmer knew data was routinely recorded to the transaction log and that he could access the data transmissions as they were being posted to the transaction log, and thereby "see" all transactions on the proprietary network. It was there, at the transaction log, that he copied account numbers and the encrypted PIN offsets onto his personal computer.

Note: While it is believed the information was copied in "real time", that is, concurrent with it being posted to the transaction log, it could have just as easily been done using another method. The programmer could have electronically copied data from the computer tape containing the transaction log and extracted the same information. Either method would have netted the same result.

At this point the programmer made a conscious decision, according to his post-arrest statement, to use account numbers from only one major bank. He said he did so because he believed that once the crime was discovered, suspicion would center on an internal problem within that bank.

After selecting a generous number of accounts from the targeted bank, the employee wrote a computer program to decrypt the PIN for each of those accounts. He was able to accomplish this using the default DES key. It was later learned that accounts from other banks were also used during the "testing" phase of the scheme and that those accounts and PINs were obtained in the same manner.

He also realized that the network would be reviewed for potential weaknesses once the crime was completed, so he reported the apparent oversight in using the default encryption key on the system and made recommendations to his superiors about how to remedy the situation. The remedies were put in place, ending his access to additional account data. He also accomplished his goal of shoring up the network so that there would be no apparent weakness in the system from which the information could have been obtained.

As an aside, it was noted by the investigating agents that the network in this case had been in operation when purchased by the communications company subsidiary. At the time of this writing it has not been established whether the default key was in use by the company from whom the subsidiary bought the network or whether a proprietary key had been in use.

Next, the defendants constructed counterfeit cards using posterboard cut to ATM card size, to which magnetic tape was mounted. The programmer then wrote a program which he used in conjunction with a magnetic encoding device "borrowed" from his office, to write the account number and other data to each of the counterfeit cards. The data was properly encoded in the appropriate positions on Track 2 of the magnetic stripe.

Among the data elements actually copied to the magnetic stripe were the Primary Account Number (PAN) and the PIN offset.

In systems where the PIN is *assigned* to a customer, the PIN is a direct derivative of the account number and the DES encryption algorithm and is referred to as a "natural" PIN. In systems where the customer *selects* his own PIN, the customer selected PIN would not match the "natural" PIN, so an offset number is used to resolve the difference. When the offset is added to the customer selected PIN, it will equal the "natural" PIN and the verification is made. Thus, in this case, an offset was necessary as the system was one in which the customers had selected their own PINs.

At the time of their arrests, the defendants were in possession of more than 7,400 account numbers with PINs and PIN offsets, all from the same bank. In fact, as previously mentioned, they were in the process of actually encoding the cards when arrested. Among the items seized during the search and arrest were the programmer's personal computer, an encoding device, and several thousand counterfeit cards in various stages of construction from uncut posterboard stock through finished, encoded cards.

Although a great deal of technology was compromised and used in the execution of this scheme, in the end this crime was one in which a trusted employee exploited his knowledge and position to manipulate and misuse the system.

The only true technical deficiency or error uncovered was that the default key was left in place when the proprietary network was absorbed. Presumably it had been in place since the system was first activated, although that has not been established as fact.

At the time of this writing, it is unknown who should have been responsible for replacing the default key with an active, proprietary key. Perhaps this oversight could have been prevented had a more thorough checklist been used by the communications company subsidiary when they absorbed the system, or by the previous owner of the network. Regardless, had the recognized protocol for securing the respective data been followed, this crime would not have been possible.

Human nature — greed, opportunity, and a willingness by the defendants to commit larceny — combined with human error in not properly installing and reviewing system safeguards account for the forming of this scheme. It is fortunate that the information came to light before the scheme was executed.

The central figure in this case is a high-school graduate and was gainfully employed with a substantial salary. He stated that he was motivated, in part, by his desire to purchase an expensive home and did not want to wait as many years as it would take to save before he could acquire the property he had in mind. His wife is a co-defendant and she too had been gainfully employed with a good salary. Another of the defendants is a graduate of the Air Force Academy and has a Masters degree from a prominent university.

None of the defendants has a criminal record. All have been charged with several counts of violations of Title 18, United States Code, Section 1029, Access Device Fraud. As written, that law provides for substantial penalties. Each count of *producing or using* counterfeit cards carries a maximum sentence of 15 years imprisonment and a fine of $50,000. The same penalties apply to the *possession of device-making equipment*. The *possession of fifteen or more counterfeit cards* carries a maximum penalty of 10 years imprisonment and a $10,000 fine.

Ultimately, upon conviction of the defendants, the recently implemented Federal Sentencing Guidelines will determine the sentences in this case. These guidelines take into account the actual and potential fraud losses in white-collar crimes such as this.

At the time of this writing, a superseding indictment is anticipated charging the defendants with multiple counts of 18USC1029.

DEFEATING TRAP TRACING

by Lord Thunder

This article should be of interest to those of you who are accustomed to receiving telephone calls by individuals who are not necessarily paying for the calls they make. Oftentimes, these people are called phone phreaks, but most of us know that a calling card does not a phone phreak make. Anyway, you receive an illegal call from someone:

Is it your responsibility to help the telephone company deal with this offender?

Do you keep track of every call you receive, when, and from who?

Should you have to deal with telephone security personnel harassing you?

Of course the answer to all three questions is 'NO' and that is what this article is all about.

Let me tell you a story.... From time to time I have been known to receive calls from telephone company security personnel asking me about who may have called me on a particular time and date. However, it seems like I can never remember and find myself unable to answer those questions. This does not mean I do not have fun antagonizing those individuals foolish enough to ask stupid questions. One incident in particular went something like this....

(The names have been changed to protect the innocent.)

R-R-R-I-I-N-N-G-G!

LT: Hello.

TA: This is Ms. Tammy Amesy from Pacific Northwest Bell, and I'm calling to find out who called you from the Portland, Oregon area at 7:43 PM on June 17, 1989.

LT: Lady... I have no idea and if I did, I would not tell you anyway!

TA: What! That person made an illegal call and if you do not tell me who it was I'll have the charges billed to your number.

LT: (Hee Hee... This idiot just screwed up bad!) Oh, ok, who is this again?

TA: Ms. Tammy Amesy of Pacific Northwest Bell.

LT: Why don't you give me your supervisor's name and number and I will speak with her.

TA: (Ah-Ha! I have him scared now [she thinks].) Sure, Lisa Algart at 503-XXX-XXXX.

<CLICK!>

R-R-R-I-I-N-N-G-G

LA: Hello.

LT: Is this Lisa Algart?

LA: Yes. Who is this?

LT: Are you Ms. Amesy's supervisor at Pacific Northwest Bell?

LA: Yes I am. Who am I speaking with?

LT: Hello. My name is Lord Thunder [No I didn't really use my handle]. Did you know that an employee of your company just committed several federal felonies?

LA: Oh my *god!* Please tell me what happened.

LT: (I explain the call to her and told her that Ms. Amesy committed extortion and fraud threats on an interstate communication carrier and also, because she was acting in the capacity as an official representative of Pacific Northwest Bell, she has left her company open to civil and criminal charges for threatening to reverse charges in order to illegally extort information from me, and I was planning on calling the Federal Communications Commission (FCC), the Public Utilities Commission (PUC), and the Federal Bureau of Investigation (FBI) to press charges.)

LA: Please, I'll talk to Ms. Amesy and make sure nothing like this ever happens again.

LT: OK, but I want something. I want a signed letter of apology from Ms. Amesy on Pacific Northwest Bell stationery.

Two days later I received the letter on Pacific Northwest Bell stationery:

"In reference to our conversation on June 23, 1989 regarding calls made to your telephone number, I apologize if you felt inconvenienced or offended. Please fell free to call if you have any questions.

Sincerely,

Ms. Tammy Amesy

Service Representative"

Now that was just one example of an attempt by the phone companies to perform trap tracing. I think code abuse is juvenile to begin with, but I do have a few things to point out on both ends.

1. Do not call someone illegally who is going to screw up and mention your name when the telephone company calls to check it out.

2. The telephone company only checks into the lengthy calls on bills with excessive costs. Keep your calls to a minimum of numbers and length to avoid being looked into.

3. Do not call relatives or personal friends that are not involved with phreaking with illegally obtained codes.

A few other things to mention. Some of the companies, like U.S. Sprint are more likely to call you up just to verify that you do not know the actual card holder. This is their way of making sure that the calls that the cardholder says are not his really are not his. I have been contacted by some of the companies (U.S. Sprint among them) a full six months after the calls were placed to answer these types of questions.

I had another interesting incident with a lady known as Julie of TMC. Some of you might remember her from a few years back. Anyway, I had been talking with a friend of mine for 45 minutes or so on a Thursday evening and on Friday afternoon I received a call from TMC Security demanding to know who I spoke with for 45 minutes the night previous. I was not about to tell them what they wanted, but it still was a little difficult to not remember who I spoke with the night before.

I whipped up a story about running an anonymous login in AE line or something. It lacked a little imagination, but it worked. Another idea you might want to try is say that you have one of those long play answering machines that does not turn off until the caller stops talking. Then mention that you had some long obscene call on there that filled up most of the tape and you wished you could find out who it was too.

So that is all I have to say about trap tracing. If you must use codes or calling cards illegally to call people, at least know how to protect yourself from security by letting your friends know what not to say when these people call to inquire.

write us a letter

Questions

Dear 2600:

Being a new subscriber, I was wondering what the 2600 represents in the title of your magazine?

Snoopy

2600 hertz at one time was a liberating cry used by phone phreaks. By sending a 2600 hertz tone down the line when connected to a long distance number, the number would disconnect and you would have total control over the long distance trunk. Not only that but billing was bypassed. This was commonly known as blue boxing. These days that method rarely works, but of course there are many others.

Dear 2600:

What steps do you take to preserve your mailing and contact list from the authorities? Is the list encrypted? Furthermore, how do you ensure against infiltration? Not that I'm the paranoid type, but this is really something you should be considering, as I'm sure the paranoid government services would be dying to get ahold of your mailing list. As a service to your clients and contacts, please keep this information secure.

There is a mail network in the works up here. I'm sure we can make arrangements for access to it as soon as a few minor security arrangements are worked out. The international flavor of this network, I am sure, as well as its constant flexibility will make it one of the most elusive and one of the most difficult to pin down from a legal perspective. I look forward to having it as one of the ways of protecting Canadian rights under the charter, and American rights under the First Amendment. Like a multinational company, this network would build capital in one of the most fundamental resources: the international protection of free speech.

JB
Ontario

Freedom of speech is not protected by hiding from the authorities. If you're trying to protect rights, then be as open about it as you can. If more people were willing to do this, we wouldn't have to be afraid.

Regarding our mailing list, don't worry. We wish we could say more, but if we did we'd be giving out the information that you want to remain confidential. We don't see infiltration as a problem. It is a two-way street, after all.

Dear 2600:

I am new to phone hacking. I sent away for plans to build a blue box (the plans they sent me are for the latest version supposedly). The box uses two 8038 intersil function generators and a 741 CV OP Amp. It has 10 25K trim pots used to tune the pole switches for the keys 1-9, KP, ST, and 2600. (The plans came from Alternative Inphormation, PO Box 4, Carthage, TX, 75633.)

Well, now that I have the thing nearly completed, one of my friends tells me that the blue box is not safe to use. He says he has heard that the phone company has equipment that can instantly pick up on the blue box and that they can get someone out to your house in minutes. This sounds like total bull to me. I was wondering if you guys knew whether or not the phone company can pick up these things that fast or not.

Confused in Kentucky

If they really wanted to, they could. But we doubt in this day and age they would really care. Unless you're from one of those rare places where blue boxing is still a problem for the phone company. Of course, if you're doing anything controversial on the phone, using your own line is not a good move.

Dear 2600:

A few weeks back I came across a number for a system in the U.S. but I can't work out how to use it.

After calling the number (1200 baud), you get nothing on your screen until you press the return key, then you are given a line saying "YALE ASCII TERMINAL COMMUNICATIONS SYSTEM v2.1" and a menu with which you select your terminal type. After this you get nothing except one line of text giving you a number to dial in the U.S. for help.

If you or any 2600 readers know anything about this system, can you please try to help with commands, etc.?

Ashley
U.K.

We suggest calling the number for help. Why not?

Information

Dear 2600:

Regarding the schematic for a device that would display a digital readout of a string of touch tones applied to its input: FI-COMMunications at 8455 Commerce Ave., San Diego, CA 92121 sells a DTMF decoder with an LED readout. It will decode all 16 touch tones. It is made to plug into the speaker output of a ham transceiver and a remote speaker can be plugged into it so the user does not lose the audio. It can be used on the telephone by modifying an old acoustical modem coupler to do what the writer wanted. The company is also working on a similar device that will have a ten digit readout with two memories, but I don't know if that is available yet. I think they sell the above device for $130 but you will have to contact them to find out.

Roy

Dear 2600:

I've read some articles about scanning for calls and want to add some information about doing so in Germany. We actually have three different car phone systems and a cordless phone system.

Carphone system B1 is frequency modulated and uses channels 1-37. Car frequencies: 148.410-149.130 Mhz. Exchange: 153.010-153.730 Mhz. Channels are in steps of 20 Khz.

Carphone system B2 is frequency modulated and uses channels 50-86. Car frequencies: 157.610-158.330 Mhz. Exchange: 162.210-162.930 Mhz. Channels are in steps of 20 Khz.

Carphone system C is cellular and has 222 channels. Car frequencies: 451.3-455.74 Mhz. Exchange: 461.3-465.74 Mhz. Channels are in steps of 20 Khz.

Carphone system D is planned for the future. It'll be in the 900 Mhz range.

Cordless phones use channels 1-40 with base frequencies of 914.013-914.988 Mhz and handset frequencies of 959.013-959.988 Mhz. Channels are in steps of 25 Khz. This system is known as Sirus.

There is also a service called TeleKarte, a German equivalent of the phone card. On the card is a microprocessor, which has stored your credit card number and a personal ID number that can be changed by the owner whenever he wants. If the owner is on a trip in the USA, he can take part in a service called "Deutschland Direct" (Germany Direct). He can call the German operator at Frankfurt toll-free under the number 800-292-0049. The operator will then ask his card number, name, credit card number, and the number to call in Germany. All costs of the call will then be charged to his credit card.

S.D.

Dear 2600:

An often overlooked place for telephone experimenters to poke around is the 811 prefix (in California). This prefix, which is used by the BOC's, holds much more than the local billing office number. From my Pacific Bell location in California I have found telco office numbers, test numbers, computers, and other things that I haven't figured out yet. Here's a sampling: 811-0317: "Testing 1234" recording; 811-0428: Pac Bell retiree services; 811-0460: computer tone; 811-1000: computer tone; 811-1212: voice computer, answers with "hello", requires numbers and access code entered by DTMF; 811-2060: computer tone; 811-298x: dead line for 10 minutes; x is 0-9; 811-3091: Pac Bell security; 811-4444: Pac Bell employee newsline recording; 811-707x: same as 298x. If you have the patience, scan all numbers in the prefix. You may want to scan during non-business hours because lots of the numbers use answering machines. These machines often identify what the number is used for. All calls to the 811 prefix are free, and many numbers are dialable from throughout the state. Happy hunting.

Mr. Upsetter

Just about every phone company outside California seems to block calls to those numbers. We do know ITT allows calls to those numbers in the 213 area code, among others. The other companies probably don't allow it because the 811 exchange doesn't look right. You can reach the numbers by using the ITT carrier access code (10488) plus the number or using the ITT calling card (950-0488). But expect to pay for a long distance call to that region. By the way, ITT is the only company we know of that provides nationwide 950 access without a surcharge. We highly recommend it and hope the other companies wake up to this valuable service.

Dear 2600:

An interesting service I just heard about: 1-900-STOPPER. $2 per minute local, $5 per minute long distance. You call it, then touch tone in the number you really want to call. Voila! You can't be caller-ID'd, as the call now originates from 1-900-STOPPER.

drop your letter in the mail

Fascinating to see how this caller ID war is shaping up.

EH

It's another rip-off that preys on people's fears. But it won't allow you to call 800 numbers, many of which have bypassed this entire caller ID debate by just doing it anyway. It's got a different name, but for all intents and purposes, nationwide caller ID is being used by a select few!

Dear 2600:

I found an interesting phone number at 212-571-3675. It seems to be a private company phone line verification and feature access point. It uses a synthesized voice to repeat back the phone number you touch tone into it.

D

That computer was floating around as a New York Telephone test number a couple of years back. Apparently the testing is over and the service is being used. We're sure it does more than repeat back the number you give it. The question is what?

Information Needed

Dear 2600:

I am writing a book about hackers and their history. As part of my research, I would like to hear from these people or people who can put me in touch with them if they are interested: Al Bell, Jim Phelps, and Tom Edison (former TAP editors), Fred Steinbeck, Bill Landreth, Joe Engressia, Kevin Mitnick, John Drake, Frank Drake, Castaalia, Aiken Drum, Midnight Owl, John Steen, Spartacus, Nick Sade, Crimson Death, Doc Telecom, Shadowhawk, Laser, The Prophet, Tom Anderson (friend of Bill Landreth), Herbert D. Zinn Jr., Lex Luthor, Knight Lightning, Erik Bloodaxe, The Mentor, Time Lord, Blade Runner, The Leftist, Adelaide, Phiber Optik, King Blotto, Phrozen Ghost, Lone Wolf, Little Silence, Captain Quieg, Unknown Warrior, Lee Felsenstein, Richard Greenblatt, Bill Gosper, Stew Nelson, Jack Kranyak, Jack Cole (the last two former editors of TEL), and any other high caliber hackers and phreaks, especially those who were active in the 70's and 80's. They know who they are! I am also interested in obtaining literature from these organizations and hearing from people associated with them: Chaos Computer Club, Phrack, Legion of Doom, and any other semi-organized group of hackers. Lastly, I would like to obtain any issues of these short-lived hacking magazines: Reality Hackers, W.O.R.M., Computel, PCC (People's Computer Company), Technology Illustrated, Journal of Community Communication, Altair User's Newsletter, Micro-8 Newsletter, Silicon Gulch Gazette, Bell System Technical Journal (years 1956, 57, 60, and 61), Syndicate Reports, and Carolina Plain Dealer. Any other information or literature which could be useful would be appreciated. I am willing to trade or purchase useful literature. Write to: Dr. Williams, PO Box 5314, Everett, WA 98206.

Complaint/Response

Dear 2600:

I am writing this letter to inform the other readers of 2600 to beware of an ad that has been running in the 2600 Marketplace for several years now. The ad I am referring to is the one that advertises TAP back issues for $100. The ad has used several names over the years such as "P.E.I." and currently is using "Pete G." The address is PO Box 463, Mt. Laurel, NJ 08054. P.E.I. or Pete G. states that "he is the original" when it comes to TAP back issues, complete with "schematics and special reports". I ordered the complete set from him awhile back for $100 and I feel I was ripped off! What Mr. Pete G. does NOT tell you is that he reduces the two inside pages of most of the issues down on the photocopier so they will fit on ONE 8 1/2 x 11 sheet of paper! I feel that I am justified in saying that about 60-75 percent of the material is NOT READABLE! It would take someone with 20/20 vision and an electron microscope to even attempt to read some of the pages! Issue #50 of TAP was a special double issue and he reduced it down on the copier and the print is not legible on about 50 percent of that issue! The so-called "special reports" he refers to in his ad are nothing more than a couple of reprints that appeared in the previous issues. I feel that anyone can charge what they want for what they have to sell, but I sure think one should be informed as to what he is actually buying also.

Rainbow Warrior

Pete G. replies: After extensive investigation, we cannot identify the Rainbow Warrior nor locate any record of a sale to him within the past two years. Therefore we will address his complaints individually.

First of all, Pete G. is and always has been me. We began advertising in the very first 2600 issue that took advertising and have been in every issue since. Purchasers were instructed to make checks and money orders payable to PEI only as a convenience so they would not have to send cash. PEI is a corporate entity which can process their checks.

Since the balance of his complaints address the quality of the copies, let me state that I have an original set which I received as a subscriber. The first issue was mimeographed in 1971 and the quality of the issues did not improve for many years. Our copies are professionally prepared. Each page is individually set for tone, size, and layout from an ORIGINAL. We cannot improve upon the existing copy, only reproduce it as faithfully as possible.

Many persons purchased copies of my TAP sets and in the following months ran ads in 2600 offering copies of my copies for other amounts of money. NONE are still advertising. It is a very time consuming and labor intensive business to prepare these copies. We are still going strong.

In closing I might add that Mr. Warrior received as the first page of his order a notice explaining our satisfaction policy and offering to replace any pages he was dissatisfied with. He NEVER advised us of any dissatisfaction with the product.

If anyone has a problem with an advertiser, please try to resolve the problem first. If you receive no satisfaction, then come to us. We will continue to run Pete G.'s ads as we see no evidence of wrongdoing.

The COCOT Article

Dear 2600:

I just received my first issue of 2600 Magazine and loved every page of it. Of particular interest was the article on COCOT's by The Plague. The article was very informative and very timely, as those vile COCOT's have started to pop up in this area in unbelievable numbers. I have a few additional ideas to add. First, instead of using the call forwarding to forward all calls to your number, why not make the COCOT forward all calls to a long distance computer? The COCOT is local to you and it gets nailed for the calls.

Another idea is to confuse the average owner of a COCOT that allows remote mode. Forward the calls from one unit to another COCOT. When the owner calls the first unit, he gets the second unit, and if done to enough of his COCOT's, it is bound to drive him nuts. My final suggestion regarding COCOT's should only be inflicted on those COCOT's that are really vicious about ripping people off. It requires the help of a friend in another part of the country who also has been the victim of a vicious COCOT. Forward all calls from local COCOT A to distant COCOT A. Then have your friend forward distant COCOT A to local RBOC phone A. Now, get an unrestricted dialtone on local COCOT B and call local COCOT A. The call will forward to the distant number, which will forward to the RBOC phone local to you. Leave COCOT B off the hook and go and answer local RBOC A. Now leave that one off the hook also. Both the local and distant offending COCOT's are racking up a large bill, and will continue to do so until some moron comes by and hangs one up. If you wanted, you could get the unrestricted dialtone on local COCOT A and place the call to the distant COCOT from there, but then you haven't screwed up as many phones as possible.

I guess if you were particularly nasty and have a lot of friends who can get their local COCOT's to get call forwarding, you could run up bills on a bunch of phones by making them all call each other. Neat, huh?

I'd like to reply to a letter written to 2600 in the same issue from Jeff. There are several ways to listen in on cellular telephone conversations. The easiest would be to buy a scanner and modify it to pick up the cel frequencies. However, if you don't want to invest in a scanner, or don't know how to make the necessary modifications, here is a neat little trick for listening in on local cel calls.

It requires two televisions with separate antennas hooked up to each UHF terminal. Put one tv on top or next to the other (on top seems to work better, but isn't always practical) and tune them both in the channel range of 75-83. Turn off the sound on one. Try different channel combinations until you find a combination which produces a different static pattern than the other combinations. You'll know when you see it. Now use the fine tuning on the one with the sound off until you hear a break in the static

2600 letters department

on the other tv. You are now in the correct area for picking up cel calls. The fine tuning will let you switch between the various cel frequencies. In my area I tune the tv with the sound off to 75 and the one with the sound on to 83. You will have to fool around with it for a while to get it to work, but once you find the proper setup, you are set forever. This little trick is why the FCC is requiring all new tv's to only go up to 74.

Halo Jones

Dear 2600:

I am writing to thank you for your excellent article on COCOT's. I am glad that someone finally told how it really is.

Recently I was a victim of a collect call placed from a COCOT. I was charged close to thirty dollars for a 10 minute call. The offending company was "Operator Assistance Network". I quickly called my local phone company and had the charges deleted. But I'm sure many other people who get victimized by such rip-offs don't do anything about it.

Taking the suggestion from the article's author (The Plague), a group of friends and myself have formed a neighborhood patrol called C.O.P. (COCOT Obliteration Patrol). By the name, I'm sure you can figure out what we do. To date we have eliminated about 65 COCOT's, and only three of those have been repaired. We prefer to "behead" the COCOT's by removing the handset, thus innocent people are NOT ripped off by dropping money into an otherwise dead phone. Our neighborhood is now almost free of these evil phones and C.O.P. will not rest until all COCOT's are out of commission.

Dan
Denver, CO

This isn't quite the way to go about it. All COCOT's are not necessarily bad. To assume they are is to write off an entire branch of technology because of a few bad experiences. Ripoffs should be eliminated. But COCOT's can actually do some good if they improve upon the service already available. It's up to us to see that they do.

Dear 2600:

You've been duped! Your article in your Summer 1990 issue entitled An Introduction to COCOT's was either (a) written by a representative of one of the local exchange carriers or (b) your writer (The Plague) has been receiving some awfully poor information regarding the pay telephone industry.

The real pay telephone rip-offs are not the independent pay telephone companies, most of which are small, independent businesspeople such as ourselves. The real rip-offs are the major local exchange carriers who subsidize their pay telephone operations with regular telephone revenues. Every one of us pays extra in the form of higher local telephone bills to support the L.E.C.'s inefficient, unresponsive pay telephone bureaucracy. Why should your home and business telephone charges support your L.E.C.'s operations?

This is not to say that there haven't been abuses in our industry. But the vast majority of us deserve better than you've shown us. Your article plays right into the monopolistic L.E.C.'s hands, who would like nothing better than to eliminate all competition and return to the days of total uncontrolled monopoly.

R.S. Gruez
Executive Vice President
American Public
Telephone Corporation

It only takes a few rip-off COCOT's to give the entire industry a bad name. We think it's important to clearly label those companies that are engaged in ripping off the public. You should do the same and disavow yourself of those companies. There need to be some basic standards introduced (equal access, 950 access, clear rate structure, etc.). We hope to hear more from your perspective and we encourage our readers to tell us if they've had any positive experiences with COCOT's and AOS companies.

Dear 2600:

I have been a subscriber for the past several years and would like to congratulate you on a fine publication. Although I do not agree with your position on several subjects, I am glad that there is a responsible forum for these ideas to be expressed. I also applaud the fact that you print dissenting views. Your summer issue which has a large section on "Negative Feedback" illustrates what I am talking about.

I am as against the abuse of power by some government agencies and the predatory, if not illegal, acts by some public companies as you are. However, I believe that these acts do not justify illegal acts by individuals. Your publishing accounts of these abuses is the best way to better the situation. The malicious and illegal acts of some individuals only helps the government justify their abuses and makes things worse.

The article, An Introduction to COCOTs, describes and endorses actions which I deplore, but as I stated above I am glad that there is a place where such articles can be published. One comment that I would like to make is that the justification which the author claims for his thesis is greatly eroded by his hiding behind a fictitious name. If he thinks that his position is morally correct, he should follow the path of other contrarians by using his own name.

Guyler Magruder
Singapore

Prison Phones

Dear 2600:

If you want a caller ID ANI system, Nuts & Bolts, PO Box 1111, Placentia, CA 92670, for around $69.95 has one but it only works in areas with Caller ID. Anyone wanting a high speed DTMF monitor can buy one from Contact East at (508) 682-2000 for around $280 along with neat toys like lineman test sets, tone test sets, line aid inductive amps for tracing, and a lot more. Granted, this stuff is not cheap but remember this is the REAL thing.

As far as phreaking from inside prison, it can be done but only on non-AT&T phones. We have collect-only here, but I got around them as follows. Ours has a recording that asks you your name. When the party you are calling answers, it plays the recording and tells you to press three to accept the call. To start with, I dialed a number to a recorded message like the one at our helpful AT&T office (hal. The recording triggers the phone to accept the call. You don't state your name when asked, but bypass it by pressing a number on the keypad until the call is placed. As the call is accepted, you'll hear the recording say "Thank you for using XXX." As soon as you hear the click that kicks in the recording, you press the receiver level down for about 30 to 50 milliseconds to hang up the switching network. You'll hear the unrestricted dial tone under the finish of the thank you message. You quickly hit the 0 once for local and twice for long distance. When talking to either operator, you simply ask to be connected to a particular number because your call is not going through. Keep it simple to avoid suspicion.

C. Rebel

We left out your location because we assume you want to continue using this.

Privacy Preservation

Dear 2600:

Reading about the Secret Service's witchhunt gives urgency to the need to deal with the increasing government rage for total manipulation of people's lives, and the need for people involved in anything controversial to try to protect their privacy. The government's passion for prying into one's privacy has reached the point where one getting "controversial" mail should consider getting a mail drop. One's mail is sent to the mail drop's address and is mailed to the customer's address by the mail drop operator. Finding a mail drop that is well run, and reasonably priced can take time, but they are out there. Many of them seem to feel they are entitled to large amounts of money for cruddy service, judging from the nearly illegibly scrawled replies I've received from a number of them.

One of the best sources for mail drops is Loompanics' Directory of U.S. Mail Drops for $12.95, which is well worth the price. Loompanics' address is PO Box 1197, Port Townsend, WA 98368. They send books via UPS.

The government has adopted the stance, and the public seems to have come to believe, that the government has an inherent right to keep track of one from birth to death, and that if someone is able to "fall through the cracks", that is itself a wrong to "society", and that if only the government can keep better track of people, it can make things "the way they are supposed to be".

The ability for people to change their name existed long before the social security number came to be used as a de facto name to track people through their lives, and the right to change one's name was expressly meant to enable one to make a break with a past phase of life, or informational detritus stored on one by various entities.

Here in California, the courts have ruled that one has a right to change one's name without court process, and that court process is entirely parallel, simply to make the change a matter of official record. One can go down to any state motor vehicles department and have one's name changed simply by filling out a small piece of paper

p.o. box 99, middle island, n.y.

for a name change of one's state ID card or driver's license. However, I've found out that one's old name is stored on the state computer for retrieval whenever one is stopped by fuzz. The DMV also takes one's thumb print for a license or state ID card.

Reverend Doktor
Norman Appleton

Wiretap Clarification

Dear 2600:

Reference is made to Hunting for Wiretaps, a letter to the editor which appears on page 24 of the Summer 1990 issue of 2600.

Although I have no quarrel with his observation that the phone company is the wrong place to shop for a service that can locate wiretaps, a number of other comments made by the author of that letter cry out to be corrected:

1. He asserts that series taps are the only kind of tap used by the phone company. The most common type of transitory tap there is takes place when a telephone lineman hooks onto your line using his handset. When he does that he has two choices: TALK and MONITOR. In the TALK mode the handset is connected in parallel across the line and works pretty much like any other extension. You can talk and listen and you draw current. In the MONITOR mode you are using a capacitive tap wired in parallel across the line. You can hear because the voices of those speaking act as AC and are passed by the capacitor. No current is drawn. We are dealing with a high impedance parallel tap, not a series tap as the writer suggests. There are several other ways that bridged (parallel) taps are used. Some are hostile and others are the result of the phone company building mirror image MULTIPLES into the system ostensibly to allow for future expansion in one or another direction. What this means is that if you listen to the correct pair on the frame in your building, you can hear your neighbor's conversations and in a like manner one of your neighbors may well have a tap of your phone mounted on the frame in his building. These parallel taps were built in by the telco to give them more flexibility in assigning lines. This sort of configuration isn't always there, but it is fairly common.

2. The author talks about 12 volts on the phone lines. He should know that the voltage found on the phone lines, unless an off hook phone or tap draws it down, is between 48 and 52 volts throughout the country.

3. The author advises the reader to "put your hand on the cable and follow it out." This "procedure" suggests that the author either lives out in a tent in the middle of a desert, miles from anyone else getting phone service, or that he has never performed the service he describes. If he has a normal house or office, not too far from his telephone is a wall through which phone wires run. How, short of demolishing the premises, does he propose to put his hand on the cable and follow it out? And how does he expect to use this procedure at the intermediate distribution frame where many wires cannot be seen or grabbed without disconnecting hundreds of phones belonging to other subscribers? How does he follow his cable through a gas pressurized splice in a manhole? Assuming he had the expertise to open such a splice without demolishing it, how does he even know that he is in the right manhole, or which of the several huge black cables entering this vault through underground conduits, contains the cable pair that go to his phone?

The business of climbing the poles is also unworkable. Many of the splices are fed by two or three cables containing hundreds of pairs of phone lines each. How does he plan to figure out which cable to hold onto? Most splices are sealed and weatherproofed. How, without demolishing the splices does he plan to get in and inspect them and follow his own phone line out? Many of the splices are located many feet from the telephone pole. Does he plan on going hand over hand along the huge black cable and dismantling the sealed splice with one hand as he holds on with the other? And what happens when he comes to a black box mounted on the ground or on a pole? Assuming he has the special key and a can wrench to open these, which of the hundreds of hidden prewired terminations go to his phone as it enters this panel and which of the hundreds of identical orange and white jumpers go to his service as it leaves the panel?

The author says that "the best solution is to have the phone disconnected and not use it at all." After going through all that work to see if his line was clean, who could blame him for switching to signal mirrors and tom-toms?

Certainly it is possible to conduct a competent sweep of the phone lines for taps, but not by using the procedures outlined by the author. In fact, the procedures he outlines virtually assure the would-be wiretapper that he will never get caught.

Alan M. Kaplan
Attorneys' Investigative Consultants
Las Vegas

A Modern Proposal

Dear 2600:

Having received your Spring 1990 issue, I immediately perused it. The articles on the harassment, arrests, etc. of hackers and phreaks disturbed me.

Because of this, I would like to put forth a proposal for debate within this magazine. In Irwin Strauss's book "How To Start Your Own Country", a small country known as Sealand is cited. Sealand is located near the mouth of the river Orwell in the English Channel. Pirate broadcaster Paddy Roy Bates laid claim to some WW2 vintage gun towers, which are very similar to offshore oil platforms. I believe it would be possible, with backing, to purchase either a boat, ideally a decommissioned oil tanker, or an older offshore oil rig, anchor it in a relatively protected area in international waters, say, in an unclaimed atoll or some such. It could then be used as a hacker/data haven, or a hacker freeport.

If there is enough interest, I may attempt this in the future.

Dr. Deviant

We had some pirate radio people try this near us a few years ago. They were in international waters, but they still got nabbed. The sad fact is that the U.S. government can and will go anywhere to stop you if they feel they have to. But there's nothing wrong with trying it anyway.

Neidorf Defense Fund

Dear 2600:

I enjoyed reading your interview with Craig Neidorf in the summer edition of 2600. I was also dismayed when I read that the EFF was not planning on funding his defense. For some reason, I had thought that defending people against governmental abuse was what the EFF was all about.

I was also disappointed that 2600 did not publish the address of the Craig Neidorf Defense Fund. I, for one, would like to send the guy a check to help him with his attorney fees. There are a few others in the BBS community out here on the West Coast who would like to help.

Jeff Hunter and
The Temple of the
Screaming Electron

We hate to disagree with our readers but we did print the address on page 40. Here it is again: Neidorf Defense Fund, Katten, Muchin, and Zavis, 525 West Monroe St., #1600, Chicago, IL 60606-3693, Attn: Sheldon Zenner. So far, contributions from our readers have been pretty dismal. If you made a contribution and you didn't get a personal thank you from Craig, let us know. If you'd rather make the donation through us, we'll be happy to forward it to him. But please do what you can as this battle is being fought for all of us.

Which Decoder Chip?

Dear 2600:

I enjoyed the Spring 1990 issue immensely. The DTMF decoder project was just what the doctor ordered. Would a more commonly available CD22204E tone decoder chip be a good substitute for the SSI202? The physical pinout is different but it seems to be electrically equivalent. For another excellent source of electronic parts, get a catalog from Circuit Specialists, PO Box 3047, Scottsdale, AZ 85271-3041.

Finally, here's a COCOT number to try: 216-928-6790. After two or three rings it answers with a female computer voice saying "thank you" followed by four touch tones.

Akron, Ohio

We're told the SSI202 is available at Radio Shack. You can't get more commonly available than that. Try these COCOT's at 212-268-7538 and 212-268-6129. Hitting a 0 will turn on a microphone and allow you to hear street noise in New York City. Or maybe a drug deal on the neighboring phone.

General Observations

Dear 2600:

For my fellow readers' info it might be important to know that beige boxes are still very available at airports. The courtesy phones that summon local motels, rental car companies, etc. are more courteous than one would imagine. The best protection I've found so far is a small speed dial box under the set connected with a simple modular

(continued on page 40)

CONVERTING A TONE DIALER INTO A RED BOX

by Noah Clayton

A very simple modification to Radio Shack pocket tone dialer part #43-141 ($24.95) can make it into a red box. The modification consists of changing the crystal frequency used to generate the microprocessor's timing. To make this modification you will need a Phillips screwdriver, a flat bladed screwdriver, a soldering iron, a pair of long nose pliers, a pair of wire cutters and a 6.5536 MHz (megahertz) crystal.

Orient the dialer with the keypad down and the speaker at the top. Remove the battery compartment cover (and any batteries) to expose two screws. Remove these two screws and the two on the top of the dialer near the speaker. There are four plastic clips that are now holding the two halves of the dialer together. Push on the two bottom clips near the battery compartment and pull up to separate the bottom part. Now slide a flat screwdriver into the seam on the left starting from the bottom and moving towards the top. (You may have to do this on the right side as well.)

When the two halves separate, slide the speaker half underneath the other half while being careful not to break the wires connecting the two. Locate the cylindrical metallic can (it's about half an inch long and an eighth of an inch in diameter) and pull it away from the circuit board to break the glue that holds it in place. Unsolder this can, which is a 3.579545 MHz crystal, from the circuit board.

The hard part of this modification is getting the new crystal to fit properly. Bend the three disk capacitors over, as indicated on the diagram, so that there will be room for the new crystal. Also remove the indicated screw. Since the 6.5536 MHz crystal you have is probably much bigger than the crystal you are replacing, you will need to bend the leads on the new crystal so that they will match up with the pads on the circuit board. Place the new crystal on the circuit board using the diagram as a guide. Solder the new crystal in place. As an added touch you might peel the QC sticker off of the PC board and place it on top of the crystal. Now carefully snap the two halves back together while checking to make sure that none of the wires are getting pinched or are in the way of the screw holes. Put the case screws back in and insert three AAA batteries into the battery compartment.

Your dialer is now ready to test. Switch the unit on. The LED on the dial pad side should be lit. Set the lower slide switch to STORE mode. Press the MEMORY button on the dial pad. Press the * key five times. Press the MEMORY key again and then press the P1 key. A beep tone should be heard when any key is pressed and a long beep should sound after the P1 key has been pressed to indicate that the programming sequence was performed correctly.

Switch the unit into DIAL mode. Press the P1 key, and five tone pulses that sound remarkably like coin tones should come out of the speaker. I usually program P1 to be four quarters (insert one or two PAUSE's between each set of five tones), P2 to be two quarters, and P3 as one quarter.

Of course, you can no longer use the unit to generate touch tones.

History and Theory

A friend of mine and I were sitting around his house one day trying to come up with a way to build a reasonable red box. I had built one with analog sine wave generators in the past, but it was difficult to adjust the frequency of the outputs and keep them accurate over time and with changes in temperature. The electronic project box I had assembled it in was bulky, hard to conceal, and definitely suspicious-looking.

My friend was playing with his calculator while I was wishing that we had the money and time to design a microprocessor-controlled device with its own custom PC board. After a while, he announced that he had an idea. He had been looking at a data sheet for a DTMF (Dual Tone MultiFrequency aka touch tone) generator chip. He calculated the ratio of the coin tone frequencies of 1700 Hz and 2200 Hz to be 0.7727. He then went through all of the tone pairs used for DTMF, calculating each of their ratios. He discovered that the ratio of the tone pair used for * was very close to the ratio for the coin tone frequencies. This ratio, 941/1209=0.7783, differed from the coin tone ratio by less than one percent.

What this meant was that since the tones generated by such a chip are digitally synthesized from a divider chain off of a reference crystal, if one changed the reference crystal to the "right" frequency, the coin tones would be generated instead of the DTMF *. Most DTMF chips use a TV color-burst crystal with a frequency of 3.579545 MHz. To determine the crystal frequency that would generate the coin tones, one would compute 3,579,545 / 941 * 1700 = 6,466,766; 3,579,545 / 1209 * 2200 = 6,513,647; (6,466,766 + 6,513,647) / 2 = 6,490,206 MHz.

Unfortunately, this is not a standard crystal value and getting custom crystals made is a real pain for the hobbyist. The closest standard frequency I could find was 6.5536 MHz. I tried a crystal of this value and it worked.

(The actual frequencies produced by a DTMF generator chip depend on the particular manufacturer's design. The color-burst crystal's frequency is divided down to the DTMF tones by an integer divider chain. Because the color-burst crystal's frequency is not an integer multiple of the DTMF tones there will be a small difference in the frequencies produced from the standard.)

When we first tried this, we were using one of Radio Shack's earliest tone dialers. It consisted of a DTMF generator chip only, and as such could not produce a sequence of tones automatically. Tones were generated as long and as fast as

Red Box Conversion

one could press the buttons. We were able to simulate nickels using this device but doing so was fairly slow and tedious. Because our manual timing was so far off of the mark, our attempts at producing dime or quarter signals were a miserable failure. A live operator would be instantly connected to the line whenever we tried it.

The Shack's next model had a microprocessor and a tone generator in it, each with separate crystals controlling their respective timing. It was just a matter of changing the micro's crystal to get the right on-off timing for a quarter's timing for a quarter's tone sequence as well as the tone generator's crystal to get the proper coin frequencies.

Later Radio Shack came out with the model used in this project. I promptly bought one because it was lower cost and more compact than their older model. I put some batteries in it and tried it out. It generated DTMF sequences with very long on and off times, but other than that, seemed like a nice unit. Upon disassembling it though, I became unhappy. There was only one crystal. It controlled the timing for a microprocessor that was specifically designed to synthesize DTMF. There was no way to independently adjust the output frequency of the tones from their on-off timing. I was just about to say, "Oh well, yet another tone dialer for my collection" when it hit me. Why not try the higher frequency crystal? The timing might come out close enough to simulate either a quarter or a dime. I made the mod and tested it out. It worked!

Thank you Radio Shack, for giving us a convenient to use, easily concealable and non-suspicious-looking red box.

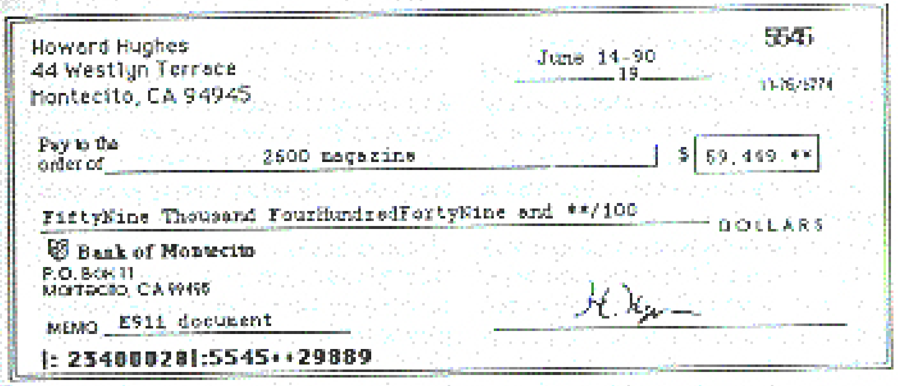
Reference

The crystal is available from Fry's Electronics in Freemont, CA for $0.89 plus the charge for UPS Red or Blue. Their number is 415-770-3763. I would suggest buying five, some for future use and some just in case you cut the leads too short when trying this project.

Coin frequencies: 1700 Hz and 2200 Hz +- 1.5%.

Timing: 5 cents, one tone burst for 66 ms (milliseconds) +- 6 ms; 10 cents, two tone bursts each 66 ms, with a 66 ms silent period between tones; 25 cents, five tone bursts each 33 ms +- 3 ms with a 33 ms silent period between tones.

Nothing gives us more joy than seeing really interesting things show up on our fax machine. If you want to send us articles, clippings, letters, pictures, or anonymous information, why not fax us at (516) 751-2608? It's the nineties thing to do.



Howard Hughes
44 Westlyn Terrace
Montecito, CA 94945

5545

June 14-90
19

11-76/1274

Pay to the order of 2600 magazine $ 59,449 **

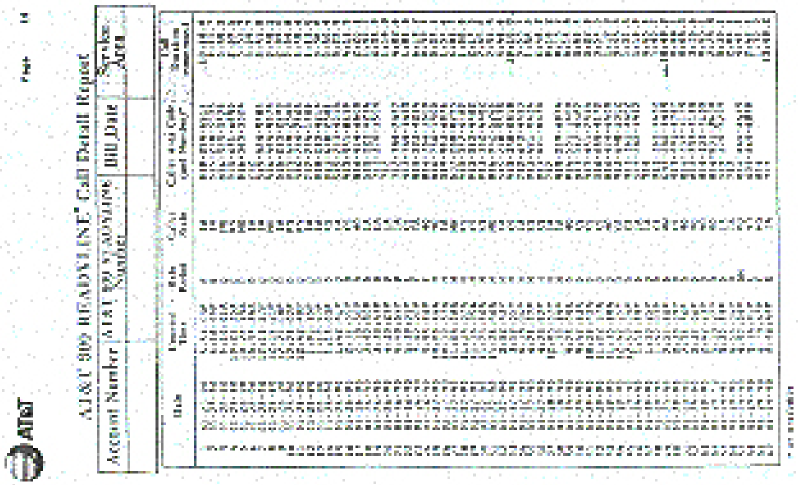
FiftyNine Thousand FourHundredFortyNine and **/100 DOLLARS

Bank of Montecito
P.O. Box 11
Montecito, CA 94495

MEMO E911 document

|: 234000281:5545••29889

We want to thank everyone who took advantage of our Spring 1990 BellSouth E911 document offer. Now we really need you to help by contributing to the Neidorf Defense Fund. Details are on page 31.



AT&T
Page 14
AT&T 800 READYLINE® Call Detail Report
Account Number
AT&T 800 READYLINE Number
Bill Date
Service Area

Here we see what many 800 customers are now able to see: YOUR telephone number. There are still parts of the country that don't pass along ANI; they are shown as area codes only.

building a telephone induction coil

by 1000 Spiderwebs of Might

This multipurpose induction coil slips over the handset receiver of any payphone or standard desk phone and can be used in conjunction with a Walkman-type cassette unit for a variety of record and playback functions with excellent fidelity — at least to the extent that the telephone lines can carry frequency response-wise. You'll need a piece of brown corrugated cardboard from the side of a discarded box, some thin cardboard (like from a cereal box), a sharp hobby knife, electrician's tape, white glue or a hot glue gun (it'll speed construction a great deal) and 50 feet of #26 wire.

Begin by taping a single layer of cereal box type cardboard (about 1/2" wide) around the receiver side of the handset and secure it with a single wrap of tape. This is a spacer layer and is eventually discarded but insures the finished induction coil slides easily over the handset's receiver. Now wrap a single layer of 1/2" wide corrugated cardboard around this spacer layer and secure with a wrap of tape. Corrugated cardboard makes the best coil form because of its strength and rigidness.

Pull the corrugated cardboard ring off and discard the inner spacer ring (or save it if you are constructing more than one coil). Glue the corrugated cardboard ring to a 4" square piece of corrugated. After the glue sets, carefully cut out the inside of the ring with a sharp hobby knife to make a nice round hole that easily slides over the handset's receiver. Now glue another 4" square piece to the other side of the coil form and again cut out the inside of the ring.

Measure out about 50 feet of #26 wire and wind it around the completed corrugated coil core. Secure the two wire ends of the coil by twisting them together a few times. At this point you can either solder a short piece of shielded cable attached to an inline RCA phono jack or a longer cable terminated with a miniature stereo plug of the kind used in Walkman-type headphones. Connect the left and right channel inner conductors together for one connection to the coil and use the shielded braid for the other connection. If possible use a coil cord. They don't tangle as easily plus coil cords always have a cool hi-tech look to them.

Now carefully trim down the outside cardboard sides of the coil and wrap a long continuous overlapping spiral layer of electrician's tape around the remaining "doughnut" coil. Make sure the finished coil easily slides over the handset's receiver without being too loose or wobbly. Add another partial layer of tape if necessary to snug up the fit. For the ultimate finishing touch the completed induction coil could be dipped in "Plasti Dip" instead of using the insulated tape. It dries to a smooth uniform rubberized coating. "Plasti Dip" is usually used to dip screwdriver, wrench, or other tool handles in order to prevent corrosion and provide a better grip.

Make a Red Box Tape

The easiest way to make one by yourself is to find two payphones side by side (like at a shopping mall, airport, or hotel lobby). Plug in your induction coil to the tape recorder's external mic input making sure you've installed fresh batteries. Pick up phone #1, slide on the induction coil (it's best to cover the mouthpiece with a thick cloth to block any extraneous sounds), start the recording mode and initiate a call to neighboring payphone #2. Answer it, press the mouthpiece against your chest to block out any noise and *slowly* deposit about $5 or $6 worth of quarters into payphone #2. Hang up phone #2 after the last coin and all your change will come back via the coin return after a few seconds delay. Now you have a red box tape of quarter tones ready to go.

Plug the induction coil into the earphone output jack of your tape recorder. Play back the series of tones — you'll hear them clearly reproduced through the earpiece. Adjust the volume control for a nice and clear reproduction. Usually the control will be a notch or two short of full volume. Now make a test long distance call to check out your new tape. Just don't let your batteries run down too low and you'll always get consistently good results. The tape can even be copied over to another Walkman-type recorder using an appropriate patch cord. It's best to record and play back the copied tape on the same cassette recorder because exact tape speed is important to keep the pitch of beep tones identical. If you want to play music or a prerecorded spoken message over the phone the induction coil will produce superior fidelity compared to the carbon mic element in the handset. While music fidelity isn't great over the rather limited frequency range of phone lines it's still OK — much better than you're used to hearing and at times it's fun to be able to do it conveniently. Since the induction coil couples all signals to the phone line via a magnetic field the fidelity is as good as possible and is only limited by the characteristics of the particular phone circuits.

(Turn page for pictures.)

STAFF

Editor-In-Chief
Emmanuel Goldstein

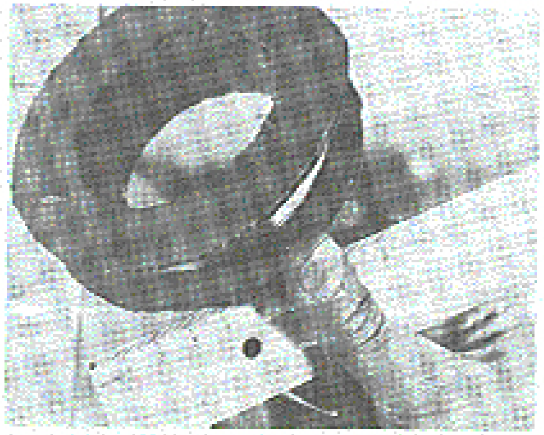
Artwork
Holly Kaufman Spruch

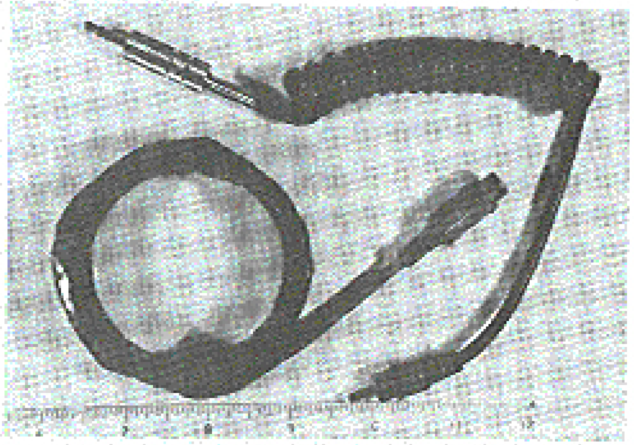
Writers: Eric Corley, John Drake, Paul Estev, Mr. French, The Glitch, The Infidel, Log Lady, Craig Neidorf, The Plague, The Q, David Ruderman, Bernie S., Lou Scannon, Silent Switchman, Mr. Upsetter, Violence, Dr. Williams, and the unusual anonymous bunch.

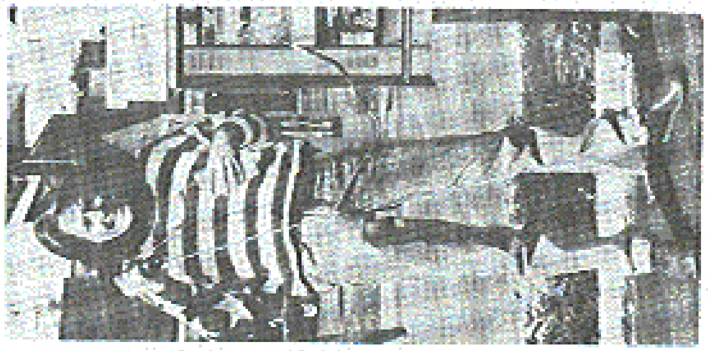
Remote Observations: Geo. C. Tilyou

Shout Outs: Steve for getting us through the last year, Franklin for the future, the electronic underground for refusing to die, and M.O.D. for continuing to allow us at their meetings.

the telephone induction coil







THE DEFINITIVE ANAC GUIDE

This is a numerical list of ANAC numbers for the United States. Dialing this number gives you your telephone number. If you don't see your area code here, try searching for your ANAC number and let us know when you find it. If you're having trouble using an ANAC listed below, try putting a 1 in front of it. If that doesn't work, the number may have changed or may not apply to your area.

205:::908-222-2222
212:::958
213:::114
213:::1223
213:::61056
214:::970-xxxx
215:::410-xxxx
217:::200-xxx-xxxx
217:::290
305:::200-222-2222
309:::200-xxx-xxxx
309:::290
312:::1-200-5863
312:::200-xxx-xxxx
312:::290
313:::200-222-2222
317:::310-222-2222
317:::743-1218
401:::222-2222
403:::908-222-2222
404:::940-xxx-xxxx
407:::200-222-2222
408:::300-xxx-xxxx
408:::760
409:::970-xxxx
414:::330-2234
415:::200-555-1212
415:::211-2111
415:::2222
415:::640
415:::760
415:::760-2878
415:::7600
415:::7600-2222
502:::997-555-1212
509:::560
512:::200-222-2222
512:::970-xxxx
516:::958
517:::200-222-2222
518:::997
518:::998
602:::593-0809
602:::593-6017
602:::593-7451
604:::1116
604:::116
604:::1211
604:::211
612:::511
615:::830
616:::200-222-2222
617:::200-xxx-xxxx
617:::220-2622
618:::200-xxx-xxxx
618:::290
713:::970-xxxx
714:::211-2121
716:::511
718:::958
806:::970-xxxx
812:::410-555-1212
815:::200-xxx-xxxx
815:::290
817:::211
817:::970-xxxx
906:::200-222-2222
914:::1-990-1111
914:::99
914:::990
914:::990-1111
915:::970-xxxx
919:::711

11953-0099

(continued from page 31)

Jack IDFWI. Others seem to be wide open and unrestricted to the world if you have a standard tone generator or can sing perfect pitch.

I have a PC with a modem but the only system I've been able to explore is the random interaction of a Wicom cordless telephone activated while I'm on line. The frequency sends garbage all over my screen and then the telco guys are under the street for weeks messing about with the local switches. I'm not sure if they are looking for a problem or adding new monitors to my line. All very scary stuff.

A consideration for serious hackers may be an association similar to A.C.E. [Association of Clandestine Radio Enthusiasts]. They had some sort of pool of funds to pay the FCC fines and legal fees for paid members who get caught. As the clampdown gets tighter we shall have to get more creative in our defenses.

Pirate cellular is growing fast. The programming sequence seems to be the key. I'm sure I'll have it soon. As dealers become busier, they are talking the owners through the setup procedure on the phone! Normally they are supposed to do it in the shop. I'll keep you posted.

First Phone, Integretel, and Midatlantic seem to all be using the same long distance lines these days. So when you get interrupted by an operator, they seem to have no idea whose customer you are. Access 950-1042 or 800-950-1042. Have a good go at them. They charge me 80 cents a minute to call my own call waiting!

Some other simple fun that I have had the pleasure of exploring is answering machines. An article on this subject would be easy to compose. All of the remote access codes are printed inside the cover or on a sticker on the bottom of the machine at your local department store, answering machine section. Playback and room monitor seem very harmless, while reset, OGM record, and on/off could cause you some trouble. Most of these can be hit with a general scan of the tones. An innovative application was played by teenagers calling on my business 800 lines over the weekend from different payphones and leaving messages for their friends to retrieve from any other payphone in the country. The cheapest way to stop them was to put in a very old machine without tone remote.

NB
Rhode Island

2600 Marketplace

2600 MEETINGS. First Friday of the month at the Citicorp Center - from 5 to 8 pm in the lobby near the payphones, 153 E 53rd St, NY, between Lex & 3rd. Come by, drop off articles, ask questions. Call 516-751-2600 for more info. Payphone numbers at Citicorp: 212-223-9011,212-223-8927, 212-308-8044, 212-308-8162, 212-308-8184. **Meetings also take place in San Francisco at 4 Embarcadero Plaza** (inside) starting at 5 pm Pacific Time on the first Friday of the month. Payphone numbers: 415-398-9803,4,5,6.

WANTED: Red and blue box plans/kits and assembled kits. Also, expansion cards for a 256K Compaq. Please contact Charles Silliman, 11819 Fawnview, Houston, TX 77070.

Do you have something to sell? Are you looking for something to buy? Or trade? This is the place! The 2600 Marketplace is free to subscribers! Send your ad to: 2600 Marketplace, P.O. Box 99, Middle Island, NY 11953. Include your address label. Only people please, no businesses.

TAP BACK ISSUES, complete set Iss 1-91, high quality, $50. SASE for index, info on other holdings. Robert H., 1209 N 70th, Wauwatosa, WI 53213.

WANTED: Atari ST hacking/telecom programs to trade. I have Mickey Dialer and 2 tone generation programs. Nil, PO Box 7516, Berkeley, CA 94707.

WANTED: Hacking and phreaking software for IBM and Hayes compatible modems. Wardialers, extender scanners, and hacking programs. Advise cost. R.T., PO Box 332, Winfield, IL 60190.

TAP BACK ISSUES, complete set Vol 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or First Class Mail. Copy of 1971 Esquire article "The Secrets of the Little Blue Box" $5 & large SASE w/45 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the Original!

NEW FROM CONSUMERTRONICS: "Voice Mail Hacking" ($29), "Credit Card Scams II" ($29), Credit Card Number Generation Software (inquire). More! Many of our favorites updated. New Technology Catalog $2 (100 products). Need information contributions on all forms of technological hacking: 2011 Crescent, Alamogordo, NM 88310. (505) 434-0234.

RARE TEL BACK ISSUE SET. (Like TAP but strictly telephones.) Complete 7 issue 114 page set $15 ppd. TAP back issue set 320 pages full size copies NOT photo-reduced $40 ppd. Pete Haas, P.O. Box 702, Kent, Ohio 44240.

VIRUSES, TROJANS, LOGIC BOMBS, WORMS, and any other nasties are wanted for educational purposes. Will take an infected disk and/or the source code. If I have to, I will pay for them. Please post to: P. Griffith, 25 Amaranth Cr, Toronto, ONT M6A 2P1, Canada.

WANTED: Audio recordings of telephone related material. Can range from recordings of the past and present to funny phone calls to phone phreaking. Inquire at 2600, PO Box 99, Middle Island, NY 11953, (516) 751-2600.

VMS HACKERS: For sale: a complete set of DEC VAX/VMS manuals in good condition. Most are for VMS revision 4.2, some for 4.4. Excellent for "exploring"; includes System Manager's Reference, Guide To VAX/VMS System Security, and more. Mail requests to Roger Wallington, P.O. Box 446, Leonia, NJ 07605-0446.

Deadline for Winter Marketplace: 1/1/91.

AN ALGORITHM FOR CREDIT CARDS

by Crazed Luddite & Murdering Thug
K00l/RaD Alliance!

As some of you know, the credit card companies (Visa, MC, and American Express) issue card numbers which conform to a type of checksum algorithm. Every card number will conform to this checksum, but this is not to say that every card number that passes this checksum is valid and can be used, it only means that such a card number can be issued by the credit card company.

Often this checksum test is used by companies which take credit cards for billing. It is often the first step in checking card validity before attempting to bill the card, however some companies stop here. Some companies only check the first digit and the card number length, others use this very convenient algorithm, while others continue on to check the bank ID portion of the card number with a database to see if it is a valid bank. These tests are designed to weed out customers who simply conjure up a card number. If one were to try and guess at an Amex number by using the right format (starts with 3 and 15 digits long), only about 1 in 100 guesses would pass the checksum algorithm.

Why do companies use the algorithm for verification instead of doing an actual credit check? First, it's much quicker (when done by computer). Second, it doesn't cost anything. Some credit card companies and banks charge merchants each time they wish to bill or verify a card number, and if a merchant is in a business where a lot of phony numbers are given for verification, this can become rather costly. It is a known fact that most, if not all, online services (i.e. Compuserve, Genie, etc.) use this method when processing new sign-ups. Enough said about this, you take it from there.

The majority of transactions between credit card companies and merchants take place on a monthly, weekly, or bi-weekly basis. Such bulk transactions are much less expensive to the merchants. Often a company will take the card number from a customer, run it through the algorithm for verification, and bill the card at the end of the month. This can be used to your advantage, depending on the situation.

If you trade card numbers with your friends, this is a quick way to verify the numbers without having to call up the credit card company and thus leave a trail. Also, a few 1-800 party line type services use this algorithm exclusively because they don't have a direct link to credit card company computers and need to verify numbers real fast. Since they already have the number you're calling from through ANI, they don't feel it necessary to do a complete credit check. I wonder if they ever heard of pay phones.

Here's how the algorithm works. After the format is checked (correct first digit and correct number of digits), a 21212121... weighing scheme is used to check the whole card number. Here's the english pseudocode:

```
check equals 0.
go from first digit to last digit
 product equals value of current digit.
 if digit position from end is odd
  then multiply product by 2.
 if product is 10 or greater
  then subtract 9 from product.
 add product to check.
end loop.
if check is divisible by 10, then card passed
checksum test.
```

Here is a program written in C to perform the checksum on a Visa, AMEX or MC card. This program can be easily implemented in any language, including ACPL, BASIC, COBOL, FORTRAN, PASCAL or PL1. This program may be modified, with the addition of a simple loop, to generate credit card numbers that pass the algorithm within certain bank prefixes (i.e. Citibank). If you know the right prefixes, you can actually generate valid card numbers (90 percent of the time).

```
/* CC Checksum Verification Program
  by Crazed Luddite and Murdering Thug
 of the K00l/RaD Alliance! (New York, London, Paris, Prague.)
  Permission is granted for free distribution.
  "Choose the lesser of two evils.  Vote for Satan in '92"
*/

#include <stdio.h>
main()
{
 char cc[20];
 int check, len, prod, j;
 printf("\nAmex/MC/Visa Checksum Verification Program");
 printf("\nby Crazed Luddite & Murdering Thug\n");
 for (;;)
 {
  printf("\nEnter Card Number [w/o spaces or dashes.] (Q to quit)\n:");
  scanf("%s",cc);
  if ((cc[0]=='Q')||(cc[0]=='q')) break;   /* exit infinite loop, if 'Q' */

  /* Verify Card Type */

  if ((cc[0]!='3')&&(cc[0]!='4')&&(cc[0]!='5'))
    {
     printf("\nCard number must begin with a 3, 4, or 5.");
     continue;
    }
  else if ((cc[0]=='5')&&(strlen(cc)!=16))
    { printf("\nMasterCard must be 16 digits.");
     continue;
    }
  else if ((cc[0]=='4')&&(strlen(cc)!=13)&&(strlen(cc)!=16))
    { printf("\nVisa numbers must be 13 or 16 digits.");
     continue;
    }
  else if ((cc[0]=='3')&&(strlen(cc)!=15))
    { printf("\nAmerican Express numbers must be 15 digits.");
     continue;
    }

  /* Perform Checksum - Weighing list 2121212121212121.... */

  check = 0;                       /* reset check to 0 */
  len = strlen(cc);
  for (j=1;j<=len;j++)              /* go through entire cc num string */
  {
   prod = cc[j-1]-'0';              /* convert char to int */
   if ((len-j)%2) prod=prod*2;        /* if odd digit from end, prod=prod*2 */
                          /*  otherwise prod = prod*1 */
   if (prod>=10) prod=prod-9;         /* subtract 9 if prod is >=10 */
   check=check+prod;                /* add to check */
  }
  if ((check%10)==0)                 /* card good if check divisible by 10 */
   printf("\nCard passed checksum test.");
  else
   printf("\nCard did not pass checksum test.");
 }
}
```

FACTS AND RUMORS

Over the past year there has been a great deal of publicity concerning the actions of computer hackers. Since we began publishing in 1984 we've pointed out cases of hackers being unfairly prosecuted and victimized. We wish we could say things were getting better but we cannot. Events of recent months have made it painfully clear that the authorities, above all else, want to "send a message". That message of course being that hacking is not good. And there seems to be no limit as to how far they will go to send that message.

And so we come to the latest chapter in this saga: the sentencing of three hackers in Atlanta, Georgia on November 16. The three, Robert Riggs (The Prophet), Frank Darden, Jr. (The Leftist), and Adam Grant (The Urvile) were members of the Legion of Doom, one of the country's leading hacker "groups". Members of LOD were spread all over the world but there was no real organization, just a desire to learn and share information. Hardly a gang of terrorists, as the authorities set out to prove.

The three Atlanta hackers had pleaded guilty to various charges of hacking, particularly concerning SBDN (the Southern Bell Data Network, operated by BellSouth). Supposedly Riggs had accessed SBDN and sent the now famous 911 document to Craig Neidorf for publication in PHRACK. Earlier this year, BellSouth valued the document at nearly $80,000. However, during Neidorf's trial, it was revealed that the document was really worth $13. That was enough to convince the government to drop the case.

But Riggs, Darden, and Grant had already pleaded guilty to accessing BellSouth's computer. Even though the facts in the Neidorf case showed the world how absurd BellSouth's accusations were, the "Atlanta Three" were sentenced as if every word had been true. Which explains why each of them received substantial prison time, 21 months for Riggs, 14 months for the others. We're told they could have gotten even more.

This kind of a sentence sends a message all right. The message is that the legal system has no idea how to handle computer hacking. Here we have a case where some curious people logged into a phone company's computer system. No cases of damage to the system were ever attributed to them. They shared information which we now know was practically worthless. And they never profited in any way, except to gain knowledge. Yet they are being treated as if they were guilty of rape or manslaughter. Why is this?

In addition to going to prison, the three must pay $233,000 in restitution. Again, it's a complete mystery as to how this staggering figure was arrived at. BellSouth claimed that approximate figure in "stolen logins/passwords" which we have a great deal of trouble understanding. Nobody can tell us exactly what that means. And there's more. BellSouth claims to have spent $1.5 million tracking down these individuals. That's right, one and a half million dollars for the phone company to trace three people! And then they had to go and spend $3 million in additional security. Perhaps if they had sprung for security in the first place, this would never have happened. But, of course, then they would have never gotten to send the message to all the hackers and potential hackers out there.

We think it's time concerned people sent a message of their own. Three young people are going to prison because a large company left its doors wide open and doesn't want to take any responsibility. That in itself is a criminal act.

We've always believed that if people cause damage or create a nuisance, they should pay the price. In fact, the LOD believed this too. So do most hackers. And so does the legal system. By blowing things way out of proportion because computers were involved, the government is telling us they really don't know what's going on or how to handle it. And that is a scary situation.

If the media had been on top of this story and had been able to grasp its meaning, things might have been very different indeed. And if BellSouth's gross exaggerations had been taken into account at the sentencing, this injustice couldn't have occurred. Consider this: if Riggs' sentence were as much of an exaggeration as BellSouth's stated value of their $13 document, he would be able to serve it in full in just over two hours. And the $233,000 in restitution would be under $40. So how much damage are we really talking about? Don't look to BellSouth for answers.

In early 1991, the three are to begin their sentences. Before that happens, we need to reach as many people as possible with this message. We don't know if it will make a difference in this particular case if the general public, government officials, and the media hear this side of the story. But we do know it would be criminal not to try.

***

When we needed to get the word out on the Neidorf story, we learned something about the power of electronic communications. By making use of the Internet, the story spread throughout the globe rapidly and responses poured back. One computer system in particular, The Well, located in the Bay Area of California and affiliated with The Whole Earth Review was an instrumental tool in opening those communications. We hope to see many other affordable multi-user systems that offer lively discussions and useful services in the future. We encourage our readers to get involved in this technology before participation in it becomes regulated and restricted by those who don't appreciate it. You can register online at The Well by calling 415-332-6106.

***

In another tale of nobody really knowing what's going on, two teenage brothers were arrested in November and charged with causing $2.4 million worth of damage to a voice mail system. It seems that the kids were promised a poster with their subscription to Games Pro Magazine. When they didn't get it after repeated complaints, they figured out how to get into the company's voice mail system. They were able to get into 200 different mailboxes, including that of the company president. The company accuses the brothers of wiping out messages, changing passwords, and changing user names. A company official expressed surprise that they were able to change names, claiming that it was not an easy thing to do.

If, as has been reported, the voice mail system was Rolm's Phonemail, the company is almost totally responsible for what happened to them. Phonemail allows passwords to be up to 24 digits in length. These clowns apparently left their passwords as the default, which is usually a mere three digits. Hence the ease of entry. And the fact that the system administrator left his/her password as the default explains how they were able to change user names so easily. A child could do it.

Not many people will claim that what these kids did was acceptable. But the way the authorities handled this was absurd, at best. Kids have always done mischievous things and they always will. And no matter how hard the authorities try, they're not going to find any conspiracy here. These were kids being naughty and taking advantage of incompetence. A stern warning would undoubtedly have put an end to it. Instead, they're being charged with all kinds of federal crimes and told that they caused $2.4 million in damage. And the U.S. Secret Service and the New York State Police seem real proud of this.

***

Speaking of the New York State Police, according to a report from the news service Newsbytes, Donald Delaney, New York State Police Special Investigator, admits to spying on 2600 meetings at the Citicorp Center in New York City. Spies working for him took pictures of people as they attended the monthly gatherings. It seems pretty absurd that they would waste their time sneaking around when we're having a public meeting right smack in the middle of midtown Manhattan. Add to this the fact that we discovered them doing this back in the spring (see Spring 1990 issue) and one gets the distinct impression that these folks haven't yet found their niche in society.

***

In a typical case of jumping on the bandwagon, a New York therapist is attempting to get some new clients out of a recent hacker story. "According to Jonathan Berent," his press release reads, "director of Berent Associates Social Therapy Center in Great Neck, NY, [the story of ZOD, a recently raided hacker] illustrates classic symptoms of social phobia — defined as the extreme fear and avoidance of people outside of one's immediate family. Mr. Berent explains that "social phobics often turn to computers in an attempt to create a substitute for the social interaction with friends that they find lacking in their daily lives. Additionally, they frequently exhibit denial — they deny that any social problem exists. They claim that they have plenty of friends — but just choose to spend their free

FACTS AND RUMORS

time with the computer instead of peers. Other characteristics of social phobia include fear of people, anxiety attacks in social situations, overdependence upon parents, difficulty with social skills, and family chaos. Another key characteristic of social phobia is anger coupled with destructive behavior. This may explain the $250,000 worth of [completely unsubstantiated as usual] computer system damages that ZOD has been accused of.'

"According to Mr. Berent, social phobia often leads to addictive behaviors -- including addictions to computers, telephone party lines, television -- even addiction to avoidance itself. Far from a mere passing phase, Jonathan Berent explains, 'Social phobia has a tendency to get worse and worse if left alone. Fortunately, however, it has been proven that social phobia is a controllable and curable problem. In our program of individual and social group therapy, we have seen countless recoveries from social phobia through clients' learning first to control their anxiety, and then learning the specific social skills that underly social success. Through goal-oriented therapy and programs that offer an opportunity for social practice, we have been able to help facilitate social phobics in breaking through their self-imposed limitations to form quality relationships — often for the first time in their lives — and live much happier lives as a result.'

"Mr. Berent has been working with social phobics for over 10 years."

Imagine that. A cure for hacking. Will wonders never cease?

***

Last issue we printed a number that read back whatever phone number you were calling from, nationwide. Our readers found this useful for payphones, tie-lines, airplane phones, or any situation where knowing the telephone number they were using was important or just interesting. Unfortunately that number has stopped working. But a new number has surfaced: 800-933-3258....Wisconsin Bell is the latest of the phone companies to drop the charge for touch tone service. We won't rest until they've all been eliminated. Speaking of rate changes, New York Telephone asked the state Public Service Commission for an $831.7 million (13 percent) rate increase earlier this year. Many people were outraged by this request. So, apparently, were the PSC administrative law judges, who recommended a rate increase of only $23.6 million (0.37 percent). In fact, after reports surfaced of wild NYNEX sex parties as well as other unethical business practices, the PSC decided to explore the possibility of forcing New York Telephone to divest itself from NYNEX. Not all public servants keep their heads in the sand, something these companies ought to keep in mind....With regards to rip-offs: did you know it costs less to call an international sex line than it does to call a local one? That's right, we saw advertisements for sex lines in the Netherlands Antilles (011-599-2424, 2626, and 6262) right next to all of those other ads. The ironic thing is that most people see the 011 and figure the call will cost more. Guess again....Both Sprint and AT&T are offering free fax services related to the Gulf Crisis. By calling Sprint at 800-676-2255 you can direct a fax update to any fax machine in the country. And AT&T is offering Desert Fax. By going to an AT&T Phone Center and filling out an official fax form, you can have that fax sent to anyone in active duty in the Gulf. They won't tell us how exactly they do it. Sorry....AT&T is accusing MCI of stealing 90,000 customers over the last six months. Nothing new there, but according to Reuters, there's now a name for this practice. Changing a customer's long distance service to another company without permission is called "slamming". Would we lie?...Finally, a light-hearted story: in early November, police in Montgomery County, Alabama were testing the new E911 system. The dispatcher received ten consecutive calls from the home of Linda and Danny Hurst. When the police arrived at the Hurst house, the culprit was soon found: an overripe tomato. The tomato was hanging over the telephone in a wire basket, dripping juice into the couple's answering machine. Apparently the juice got into the machine's dialing system and caused it to dial the police. "We're not sure how," Chief Deputy Milton Graham said. "Maybe they had speed dialing and it shorted out." Linda Hurst also was baffled. "I didn't know the answering machine could even dial out. It's just supposed to take messages."

DON'T MAKE THAT MISTAKE

Many people do. They intend to renew, but the drudgeries of daily life get in the way. And then, one day, they realize that there's something missing. You see, we don't pester you repeatedly like most other magazines when your subscription runs out. You won't get phone calls, postcards, telegrams, faxes, or knocks on your door. We accept rejection gracefully. The tragedy occurs when subscribers **forget** to renew. Go look at your address label now. If you've only got an issue or two left, renewing today makes a whole lot of sense. And by renewing for multiple years, you'll have one less thing to worry about in a decade that promises to have plenty of worries.

INDIVIDUAL SUBSCRIPTION

□ 1 year/$18 □ 2 years/$33 □ 3 years/$48

CORPORATE SUBSCRIPTION

□ 1 year/$45 □ 2 years/$85 □ 3 years/$125

OVERSEAS SUBSCRIPTION

□ 1 year, individual/$30 □ 1 year, corporate/$65

LIFETIME SUBSCRIPTION

□ $260 (you'll never have to deal with this again)

BACK ISSUES (never out of date)

□ 1984/$25 □ 1985/$25 □ 1986/$25 □ 1987/$25

□ 1988/$25 □ 1989/$25

(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)

(individual back issues for 1988, 1989, 1990 are $6.25 each)

TOTAL AMOUNT ENCLOSED: □