2600 January, 1984!

Published monthly by 2600 ENTERPRISES, an eleemosynary organization. Subscription rates are $10 annually. Write to 2600, Box 752, Middle Island, NY 11953.

*0#D

VOLUME ONE, NUMBER ONE

AHOY!

(That's how Alexander Graham Bell used to answer his phone. For some reason, it never caught on...)

This is the very first issue of *2600*. We will, on this page, explain our motives and what the goals are which we hope to achieve with this publication.

The idea for *2600* was born early in 1983. We saw a tremendous need for some form of communication between those who truly appreciate the concept of communication: technological enthusiasts. Of course, others have different ways of describing such people—these range from words like hacker or phreaker to stronger terms such as criminal or anarchist. Our purpose is not to pass judgement. *2600* exists to provide information and ideas to individuals who live for both. **All of the items contained on these pages are provided for informational purposes only. *2600* assumes no responsibility for any uses which this information may be put to.**

Of course, a lot has changed since our first days. *War Games* came out. And then the 414 gang got caught. Suddenly everyone was talking about phreakers and hackers. And while there were some that sort of jumped into the limelight, others were a bit more cautious, in fact, some were quite upset. Sure, the publicity was fun. But what would be the cost?

Well, time has passed and the cost has been high. Phreakers and hackers have been forced into virtual isolation. Raids by the FBI have become almost commonplace. The one magazine that was geared towards phone phreaks (*TAP*) mysteriously disappeared at the height of the crisis, sparking rumours that they, too, had been raided. However, in November, the magazine resurfaced, with an explanation that a fire had destroyed part of their mailing list. (Incidentally, if your name was one of the ones that was lost, you can claim the issues you are entitled to by sending *TAP* a copy of their mailing label or a cancelled check.)

And then there was the legendary computer bulletin board known as *OSUNY*. Enthusiasts from all across the country called up this board and left messages ranging from the latest in Sprint codes to how to crash an RSTS system to what to do once you've finally gained access to Autovon. Within a week after being mentioned in *Newsweek*, *OSUNY* was disconnected. Word has it that they are still in existence somewhere, but by invitation only. A truly smart move, if that is the case.

Many hackers were keeping a low profile even before the October raids. When the FBI confiscated equipment from 15 sites across the country on the twelfth and thirteenth of the month (sponsored by a grant from the folks at GTE), many of our contacts were lost because they feared the consequences of continuing. Two organizations, the Inner Circle and PHALSE, were deeply affected by the raids. The latter group (whose initials signify Phreakers, Hackers, and Laundromat Service Employees) is still in contact with us on occasion and has promised to contribute many articles devoted to just what was really going on.

So it seems that the events of 1983 have conspired to actually *strengthen* the resolve of hackers and phreakers across the country to put out this monthly newsletter. We hope you will help us continue by subscribing, spreading the word among your friends, and of course contributing articles and information. Since we are non-profit, it really doesn't matter to us if you xerox your copy and send it to someone else—all we ask is that you let us know so that we can have a rough idea of how many people we're reaching.

2600 has several sections, some of which will appear every month, others on an irregular basis. On this, the front page, and on page two, you will always find informative full-length features on relevant subjects. Future topics include: "A Guide to Long Distance Telephone Services and Their Vulnerabilities", "DEC and Their Many Mistakes", "Phreaking in the Sixties", and "Tracing Methods Used by the Law", as well as any late-breaking items. "FLASH" appears on page 3 and provides a roundup of timely news items written from a technological enthusiast's perspective. Page 4 is used for a variety of things—interesting stories from the past, schemes and plots that just might work, and feedback from subscribers. The last two pages of *2600* are comprised of data. Just what sort of data, we cannot say. However, if it is something that you are looking for, then you will probably recognize it.

The three holes on each page serve a purpose. We suggest that you obtain a loose-leaf book so that you can neatly file every issue of *2600* you receive.

Many thanks to those of you who subscribed without even seeing an issue. A word of advice, though: don't do it again or you'll probably get ripped off! We'd also like to thank those who took advantage of our free issue offer. If interested in subscribing, the rates and address can be found at the top of this page.

Welcome to *2600*. Turn the page and become a part of our unique world.

FBI GOES AFTER ADS HACKERS

IBM must press charges before action can be taken — Feds reveal their tactics, blow source

On this page we had originally planned to run an article entitled: ESS — Orwell's Prophecy. *At the last minute, however, we received this bombshell from an anonymous contributor. It seems that a group of hackers was making use of one of IBM's ADS systems. (Audio Distribution Systems enable users with touch-tone phones to send voice messages back and forth to each other. Look for an in-depth article on them in a future issue.) Unfortunately, as is all too often the case, one of these hackers was really an FBI informant who was taking note of all of the illegitimate users (around 40 or so). Luckily for this particular group, the informant was sloppy and left many telltale clues which gave them literally months of warning. So, when the informant decided to send a message to the system operator, advising IBM to take action against the hackers and to call the FBI for more information, the hackers were ready. The system operator's account had also been penetrated by them and hence, the message was received by the hackers first! One of them actually followed the instructions in the message and called the FBI! And for some reason, the investigator there thought he was talking to an IBM executive. This is some of what he said.*

One of the individuals that supplies me with information from time to time has uncovered a lot of abuse within the ADS systems, not only here in the United States, but in England and Italy. I talk to this individual on a private bulletin board. . .

We have no ability to come in as an outside investigative or law enforcement agency and do anything about it because, first off, we don't have a complainant. We don't want to step on anybody's toes, but it's been our policy to monitor bulletin boards and the phone phreaking activity across the country and advise commercial computer systems and corporations if we do discover certain computers along with the passwords and account numbers being published on the board. We do this on a one on one basis.

The GTE Telemail Connection

That was my baby, too! As a matter of fact, that's how we came across the ADS system — through the GTE investigation. [These] people are not just interested in data communications through terminals — they will leave voice messages on an ADS. We have been slowly uncovering more and more on the ADS in the last two months.

The major phase of [the Telemail investigation] was about 20 individuals that we had located and identified and we're looking for indictments on most of them coming down in the next month or two. We're talking about a group of highly organized people that do communicate on a daily basis all the way across the country — from San Francisco and L.A. to Denver to upstate New York. So we have a core of individuals that we are still looking at that are using your system and then we have this peripheral that we are not as concerned about because they are not part of an out & out conspiracy or an organized network, per se. I know of at least 8 or 10 that are the central figures in this, the carryover from Telemail. And we keep hearing information of other people who are calling in with junk messages — there's no real substance to their messages. Now the reason I know that is that they have included one of my sources of information onto their system and so he gets messages from the other parties.

The Communist Connection

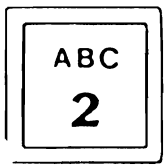
In a way we're somewhat fortunate that it's 16-year-olds or 26-year-olds as opposed to people from behind the Iron Curtain. It gives us the opportunity to see how these systems work and see if we can plug any loopholes before somebody from a not-friendly nation would try the same thing. I personally fully expect it — I'm surprised it hasn't happened in the past. It may have. We just haven't caught it. But the kids are a little bit sloppier and they're getting caught. . . I hate to sound paranoid, but we're supposed to be considering the big picture as far as is there anything sensitive in nature. For us within the bureau, sensitive in nature first off means national security and you've got corporate trade secrets and the like that you don't need being distributed.

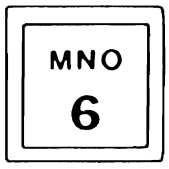
How the FBI Wins Trust and Gets Info

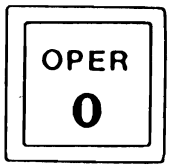
The subjects have an ego problem and they love to talk to other individuals about what they are capable of doing and bragging about it. They have a tendency to trade information. Everything is negotiable with them. We have never had to barter away access to systems — we do it more on the technical information of phone networks, computer systems, and the like to where it's more of a technical information tradeoff as opposed to an access tradeoff. [An example would be the] login procedure for a PDP-11. You integrate yourself within their confidence and their circle of friends. You feed them a little bit of bait and a lot of times they'll go for it. You enter into a dialogue with them and they end up taking you for a ride.

These people are very hungry for technical avenues through which they can communicate. It used to be the personal computer bulletin boards — public messages that anybody can read. You start finding out that they leave a phone number or an address — and you start finding out who the parties are. There's thousands of these bulletin boards across the country and you narrow in on maybe twenty or so that are the more hardcore bulletin boards that are being used for exchange of illicit information. Then they move from there to an electronic mail service, namely GTE

(Continued on back page)







FLASH

GTE raids still have many unanswered questions—computer owners concerned

Combined News Sources

On Wednesday, October 12, at 6:00 AM, the FBI started to raid the homes of over fifteen individuals for allegedly breaking into Telemail, GTE Telenet's massive electronic mail service. While much of the publicity has now died down, questions remain concerning the legality and the overall implications of such computer seizures.

At a December 16 meeting of the Long Island Computer Association, this topic was addressed. Some members could not understand the rationale for taking away the computers in the first place. "It sounds like scare tactics to me... to keep these kids off of computers," one commented. "To hold the equipment seems like something that should be unlawful and it's something that the public should look at. If it's not justified, we should say that we won't put up with it anymore and to return the equipment." He did not elaborate on precisely what kind of action a computer group such as LICA could take.

Legally, the computers can be kept for as long as they are needed in the investigation. Ultimately, a judge will decide how long that can be.

"The allegation," said an attorney familiar with the case, "is that the services of the Telemail bulletin boards were used and the theory that the government is proceeding under is that it was a violation of Section 1343, wire fraud (a scheme with intention to defraud someone else using either television, telephone, or some other communications means). They're saying that if there was use of the bulletin board service, then that was a 'theft of service' and there was intention to defraud GTE."

One member took GTE's side. "These are all nice games these people are playing, but they are a theft of service. Somebody is in the business of providing that service and they're deliberately interfering with their providing that service. They're trying to get something for nothing."

Another disagreed. "You may be on their computer, but it's not costing them anything, if you're not taking up time. Unless the whole system is fully used and you were the last user on, are you really using any of their time? Really and truly?"

Many hackers felt they were unjustly accused. One even said he'd never used the Telemail system. Others said they had looked around once or twice but had never hurt anything. Others, though, admitted to deleting mail and playing tricks, like sending obscene messages back and forth between two innocent executives.

Whether or not the Telemail system was used fraudulently did not seem to be the overriding issue at the LICA meeting. What had members there worried was the way in which the investigation was being carried out. When dealing with computers as evidence, different rules apply, rules that for the most part have not been written yet. "Data can be manufactured just as easily as it can be erased from a personal computer," one member commented. "And the longer that they have the computer in their custody, the less likely that the information that they claim is on it was actually there. Because, as we know, you could enter any date, any time into the computer and have it date- and time-stamp the files."

Meanwhile, a GTE Telenet spokesperson said that the corporation still intends to prosecute and denied that the whole thing was being put on for the deterrent effect that it might have on other people. The spokesperson also said that abuse on the system was discovered in the past, but they didn't prosecute at that time. This time, though, they're serious.

AT&T Credit Cards Make Debut

2600 News Service

There's now another way to place telephone calls without dimes. This month, the "true" AT&T credit card phones are making their debut in various airports around the country. This new phone actually takes an AT&T credit card (not those wimpy "calling cards" or "PIN cards." We're talking about a *real* hunk of plastic, with a magnetic strip and everything.) — and there's even a little video screen that gives you directions.

Unless some sort of a bug can be found within the system itself, phone phreaks won't accomplish very much here, unless they can actually get their hands on other people's cards. This, in itself, wouldn't be too difficult, since large numbers of the cards would be sent out on the same day in a particular area. Stealing out of personal mailboxes, though, is an act most phone phreaks would never stoop to. And the folks at AT&T are well aware of this.

Wireless phones spell trouble

2600 News Service

With cordless phones popping up all over the place, problems were bound to arise. It's not at all uncommon to hear another cordless conversation on your phone or to hear the electronic pulse-beeping when you're not even dialing. Then there are cordless phone phreaks to deal with, who drive into heavily populated zones holding one of the common cordless models. It's called "cruising for dialtones." And some phones are nice enough to broadcast your conversation on an AM frequency. This feature isn't very good for private conversations. It helped shape a recent drug bust in the state of New York.

Recently, a lady in the Midwest called up her local electric company to tell them that she was going to be away for two months. A member of the 2600 Club heard this on his radio and, being in a good mood, called her and told her that important, personal business should *never* be discussed on cordless phones. After thanking him, she exclaimed, "That thing's going right back to the Phonecenter Store!"

1984 arrives in Hong Kong

The Los Angeles Times

In an effort to "discourage people from driving their cars in heavily congested areas" all 350,000 of Hong Kong's motor vehicles will be fitted with tracking devices that will let government computers know exactly where each car has traveled so that the owner can be billed for road use. This system could be in full implementation by 1987, if the government has its way. Such a system would also allow the police to quickly pinpoint the whereabouts of any vehicle. Tampering with the $45 tracking devices will be illegal and any attempt to do so will trigger street cameras to photograph the license plate of the car.

THE TRUTH BEHIND THOSE 9999 NUMBERS

by Mark Bluebox

Once upon a time, I was talking to one of my favorite friends, one of the nation's oldest and most experienced telephone enthusiasts—some might refer to him as a phone phreak. In this particular conversation, he mentioned to me that I might want to experiment with a series of 800 numbers: exchanges starting with 9, followed by the suffix 9999 (800-9xx-9999). And so I did, and a whole new world began to open up in front of me.

They were mostly weather and time numbers in various locations throughout the country. And, since these were 800 numbers, there was NO CHARGE! One number in particular was of a great deal of interest to me and to many others. This was 800-957-9999, which hooked up to WWV, the radio station operated by the National Bureau of Standards that does nothing but tell the time and give shortwave reports. This is the most accurate clock in the entire world! You either have to tune WWV in on a shortwave receiver or dial 303-499-7111 in Fort Collins, Colorado. Yet, here I was with an 800 access! Being a bit of a shortwave enthusiast, I don't have to tell you how convenient this was for me. Unfortunately, it got too convenient for too many people.

I guess I made the mistake of giving it to a former president of a large amateur radio club in the Dallas area. He, in turn, printed it in the Amateur Radio Newsbulletin where thousands of people probably saw it. Another statewide newsbulletin picked it up and printed it. Through an amateur radio news network which this bulletin was a part of, the news got as far as California.

One day, I called up the West Link Amateur Radio News Service at 213-768-7333. (This is a service located in West Link, California that broadcasts news over amateur radio, VHF, UHF, etc.) Their latest report had this little item: "Speaking of interesting things, the National Bureau of Standards has got a very convenient time number for those of you that are not constantly at a shortwave receiver. You can dial 1-800-957-9999 for WWV. It's just another good toll-free service for us to use." The avalanche had really begun now.

The West Link report was heard on bulletin stations all around the world and, apparently, one station in Nashville, Tennessee broadcast it. From there it fell into the hands of one of the writers for the DX program on Radio South Africa! I happened to be listening to a program where they were talking about pulling in distant time stations, weather stations, etc. He then mentioned, "For those of you that live in the United States, a convenient toll-free 800 number has been provided by the National Bureau of Standards for WWV and that number is 1-800-957-9999." Imagine my surprise! Once again, the number had been broadcast all around the world. People in many, many nations now had that number. Of course, the number only worked inside the United States, but the word was being spread by shortwave listeners and QSL people everywhere.

The number was getting swamped. Needless to say, it was busy much of the time. A government official, who *also* had this number, thinking that it was legitimate, called up WWV and complained. He told them that they needed to add some more lines to their new 800 number. The general manager of the station said, "I don't know *what* you're talking about. I don't know of any 800 number that gets you WWV."

The government official told him what the telephone number was. The general manager called it and heard his own station. Astounded, he contacted the Mountain Bell Telephone Company in Denver, Colorado. They said, "You're not paying for any 800 in-WATS number. We show 303-499-7111 for WWV, but we don't have any 800-957-9999."

Mountain Bell checked it out and sure enough, the number existed but not on *their* records. No one was getting charged for this! Now, of course, you know a monopoly as well as I do—they're *sure* not going to let anyone have a free ride. So they told the WATS coordinator to find out what happened. He finally made the discovery that some technicians had hooked that number up for transmission testing. [These switching technicians are toll technicians, AT&T Long Lines switching technicians, and carrier systems technicians. In other words, they're the group of people who link switching centers together, from New York to Los Angeles, for example. In this case, the whole escapade was a kind of group effort. The switchmen and the carrier people got together and set up this number for testing, finding noisy carriers, carriers with cross-talk on them, etc.]

The WATS coordinator told them they'd better get this number off—too many people knew about it. He told them to erase *every* 800 test line number that was on the system. Not surprisingly, someone also got chewed out very severely.

So, consequently, 800-957-9999 is no longer in existence. But since then, less than two weeks later, several of the 800 test numbers have begun to defiantly reappear. Check around, you'll probably find a few interesting ones. But I doubt if WWV's brief stint as a toll-free service will ever be repeated.

Ahoy, folks! If any of you have ever used an extender that goes by the name of 8006213129, you'd better give it a call now! The people running it have a message for you.

DISREGARD THIS: 36TK109S7752A1453009422116YBR:

Position	Name	Extension
Office of the President		
The President	Ronald Reagan	2858
Special assistant	David C. Fischer	2168
Personal secretary to the President	Kathleen Osborne	2858
Office of the Counselor to the President		
Counselor to the President	Edwin Meese III	2235
Deputy counselor	James E. Jenkins	7600
Assistant counselor	Edwin W. Thomas Jr.	2235
Special assistant	Mitchell F. Stanley	2235
Assistant to the President for Cabinet affairs	Craig L. Fuller	2823
Secretary	Adela Gonzalez-Nardi	2823
Assistant director	T. Kenneth Gribb Jr.	2800
Administrative assistants	Karen Hart	2823
	Nancy A. (Missy) Hodapp	2800
Director of planning and evaluation	Richard S. Beal	6690
Office of Chief of Staff		
Chief of staff	James A. Baker III	6797
Executive assistant to the chief of staff	Margaret D. Tutwiler	6797
Staff assistant	Kathy Camalier	6797
Confidential secretary	Margaret Glasscock	6797
Deputy to the chief of staff	Richard G. Darman	2702
Administrative assistant	Sara Currence Emery	2702
Secretary	Janet F. McMinn	2702
Special assistant to the chief of staff	James W. Cicconi	2174
Presidential correspondence	Anne Higgins	7610
Special presidential messages	Dodie Livingston	2941
Office of the Deputy Chief of Staff		
Deputy chief of staff	Michael K. Deaver	6475
Assistant to the deputy chief of staff	Joseph W. Canzeri	2861
Staff assistant	Shirley Moore	6475
Special assistant to the President for private initiatives	James S. Rosebush	2957
Executive assistant	Bernyce Fletcher	2957
Director of special support services	Edward V. Hickey Jr.	2150
Deputy director of special support services	Dennis E. LeBlanc	2150
Deputy director of military office	Col. Frank E. Millner	2150
Army aide to the President	Lt. Col. Jose A. Muratti Jr.	2150
Air Force aide to the President	Maj. William M. Drennan	2150
Navy aide to the President	Cdr. William R. Schmidt	2150
Marine Corps aide to the President	Maj. John P. Kline Jr.	2150
Physician to the President	Dr. Daniel Ruge	2672
Director of advance	Stephen M. Studdert	7565
Deputy director of advance	Hugh L. O'Neill	7565
Administrative assistant	CeCe B. Kremer	7565
Trip desk officers	Marti J. Frucci	7565
	Karen Jones Roberts	7565
	Lynn Smallpage	7565
Advance staff	Robert K. Gubitosi	7565
	James F. Kuhn	7565
	Dan Morris	7565
	Lanny F. Wiles	7565
	Rocky D. Kuonen	7565
Director of scheduling	Gregory Newell	7560
Deputy director of scheduling	Tricia Rodgers	7560
Administrative assistant	Cristy Valentine	7560
Staff assistants	Michael Castine	7560
	Frances (Fan) Snodgrass	7560
	Netta A. Dickey	7560
Confidential assistant	Mary H. Rawlins	7560
President's diarist	Ellen Jones	7560
Appointments secretary	Helen C. Donaldson	7560
Staff directory for the First Lady	Peter McCoy	6702
Administrative assistant	Christine J. Hathaway	6702
Press secretary	Sheila P. Tate	7136
Assistant press secretary	Barbara Cook	7136
Personal secretary	Elaine Crispen	6633
Social secretary	Muffie Brandon	7064
Assistant social secretary	Linda Faulkner	7064
Scheduling director	Nina Wormser	7910
Special projects	Ann Wrobleski	7905
Office of the Vice President		
The Vice President	George Bush	7123
Executive assistant	Charles G. (Chase) Untermeyer	2587
Chief of staff	Daniel J. Murphy	6606
Deputy chief of staff	Richard N. Bond	7056
Military assistants	Lt. Col. Michael D. Fry	4213*
	Lt. Col. William Eckert	4223*
Counsel	C. Boyden Gray	7034
Deputy counsel	Rafael V. Capo	7034
Press secretary	Peter Teeley	6772
Deputy press secretary	Shirley M Green	6772
Speechwriter	Christopher Buckley	7453
Domestic policy adviser	Thaddeus A. Garrett Jr.	2173
Assistant domestic policy adviser	Mary S..Gall	7935
National security affairs adviser	Nancy Bearg Dyke	4213
Congressional relations assistant	Robert V. Thompson	224-2424
Legislative assistant	Susan Alvarado	224-8391
Assistant for appointments and scheduling	Jennifer Fitzgerald	7870

All telephone numbers are on the 456- exchange except those marked with an asterisk, which are on the 395- exchange, and those listed in full

Proper tabbing is extremely important when typing a list. Above is an example of tabs used successfully.

This here page is usually a continuation of page 5. However, when we get a blockbuster story like the one below, we have to reallocate our space. We know you'll understand. By the way, as long as we've got you looking up at this part of the page, why not take the time to send us some mail? Letters, articles, information, old telephones, paintings, anything, really. You know the address (it's on the front page). Let's hear from YOU.

FBI VS. HACKERS

(Continued from second page)

Telemail. They caused fits within Telemail when they decided to get a little bit cocky and see if they could shut down accounts and change passwords of the administrators and things like that. From there they have moved one step further to where they are now the same individuals communicating through the ADS systems and they also set up conference calls through the Bell System, so they're not just attacking one particular system or one individual avenue of communication — they try to hit them all. It's an ego trip for all of them.

Pen Registers

We would put a pen register on the phone line of the individual (suspect) and it would record only the digits dialed on his telephone — we would not use a full blown wiretap to record his voice. We can only put a pen register on an individual's phone for like, thirty days before we have to go back to a judge and try to get an extension and we try to minimize the use of our electronic surveillance equipment so the public does not think we're the Big Brother of 1984. (laughter) It's coming. Actually, we're already there! (hearty laughter)

We have not utilized any pen registers for the specific purposes of going after abusers of the ADS systems. First off, we have to have an actual case presented to us or a complaint. It's a roundabout way of doing it, but it's the way that we, in the bureau, have to have somebody outside come to us. Otherwise we can carry on the whole investigation without IBM even being aware that we are monitoring activity within their system and we don't want to become that secret police, or anything like that. We want to be above board and work with the corporations in the community.

Just How Much Trouble Are These Hackers In?

On the federal level we can prosecute them for telephone fraud (fraud by wire) if we can determine that the ADS is an ongoing business operation and that you are being denied your just revenues by them sneaking onto your system and abusing your system. The strictest penalty is a $1000 fine and 5 years in jail for an actual conviction of fraud by wire violation. Those are always lax — a more common sentence may be for an adult maybe a year in jail, 18 months, or a fine, sometimes they get probation, or agree to pay back any fraudulent money obtained or for services rendered or whatever to the client company — it stays on his record for a year, he's on probation for a year and at the end of that, his record is wiped clean. Rarely do they get the maximum penalty. It just doesn't happen.

Do Me a Favor

Please do not disclose any geographic location because we are kind of unique in that we do not have any other source available in any other part of the country that could supply us with information like this. He may be one of 200 people, but if you identify Michigan you identify between 2 or 3 individuals and it may burn the source.

We'd like to make it clear that we don't intend to do this kind of thing very often, since rumours about certain people being informants are very common in this business. But this is no rumour. This, friends, is solid fact — we would not have printed this story if we weren't able to substantiate the claims it makes, and we had no trouble at all doing that. Our intent in making this information known was not to screw up the FBI's fun (they're really not doing all that much out of the ordinary anyway), but rather to expose a very dangerous individual who goes by the name of Cable Pair (some say his real name is John Maxfield). This person has been posing as an extremely friendly hacker who lives in Detroit and is just bubbling over with technical information in exchange for your secrets. He claims to have been one of the nation's first phreaks, which may or may not be true. He gives out his telephone numbers freely, will do anything to communicate with somebody (like place conference calls from his own private PBX system, provided you give him YOUR phone number), and generally will use anything you say to him against you in the future. Our advise is simple: stay the hell away from this person. Even if you haven't done anything wrong yourself, your life can still be made miserable by him if you're even suspected of having contact with wrongdoers.

This latest turn of events has saddened us — we thought Cable Pair would be a promising contributor to this publication and instead we learned a valuable lesson: don't trust anybody. Have fun, Cable Pair. Enjoy yourself. Just don't expect to see any of us over at the Chestnut Tree Cafe with you. You're on your own now.