2600

The Monthly Journal of the American Hacker

Volume 4, Number 3 March 1987 $2

Reach Out and Touch a Nuclear Weapons Contractor

• Your local telephone company will soon be sending you a special ballot (if it hasn't done so already), asking you to pick a long-distance carrier for "dial-1" service. **Be sure to make the right choice.** Nuclear Free America is encouraging individuals, organizations and communities to join in boycotting not just AT&T but all long-distance phone companies with ties to the nuclear weapons industry.

Of the major long-distance telephone companies available in the United States, only Allnet has no ties to the Department of Defense. All the others are wholly or partly-owned by military contractors, and, of these, all but MCI and Western Union are profiting directly from the research, production or testing of nuclear weapons. Even if you have already selected a long-distance service, you can still switch to a non-nuclear alternative for a nominal charge -- usually less than $10.

For more information, write for Nuclear Free America's new flyer entitled "Reach Out and Touch a Nuclear Weapons Contractor," which profiles both the nuclear and non-nuclear alternatives available nationally. (Available for $1 from NFA, 325 East 25th St, Baltimore MD 21218.)

P.S. If you do switch from AT&T, please be sure to call or write AT&T Chairman James Olson (550 Madison Ave, New York, NY 10022; 212-644-1000) to let him know your reasons for doing so.

The Top 50 Nuclear Weapons Contractors

Allied Signal
AT&T
Boeing
DuPont
Eaton
EG&G
Emerson Electric
FMC
Ford Motor
GenCorp
General Dynamics
General Electric
General Motors
Goodyear
Gould
Grumman
GTE
Harris
Hercules
Honeywell
IBM
ITT
Litton
Lockheed
LTV
Martin Marietta
McDonnell Douglas
Monsanto
Morton Thiokol
Motorola
Nat'l Distillers
NL Industries
N. American Philips
Northrop
Penn Central
Raytheon
RCA
Rockwell Int'l.
Sanders Associates
The Singer Co.
Sperry
Teledyne
Tenneco
Texas Instruments
Textron
TRW
UNC Resources
United Technologies
United States Steel
Westinghouse

Compiled by Nuclear Free America based on Fiscal Year 1984 data from the Dept. of Defense and the Dept. of Energy.

For those of you who've been bewildered and baffled by our rather specific articles about computers and the programs that are run on them, like COSMOS, take heart. You are not alone. But, as we said last month, you don't have to understand the specifics to realize the potentials.

Our COSMOS article this month is probably as specific as we can get on the subject. But we'll continue to devote space to the many things that powerful computer applications can create—and destroy.

As always, there's more than one subject in our issue. We're quite happy to have the work of a talented folk artist featured in this month's issue. While that in itself sounds rather unusual for our publication, the subject of the poem we've reprinted, phone phreaking, certainly isn't. We think many of our readers will recognize themselves in this feature.

And for those of you who still haven't figured out how to make a long distance phone call (legally, that is), we've devoted some space to an article on equal access that was actually released last year. One or two of the companies mentioned, in fact, have since been merged. But this still ought to be a big help to anyone who's had trouble dealing with this major problem of the eighties.

As always, we welcome your letters and comments. And, since we've started sending 2600 out as second class mail, we're curious as to how long it takes to reach our readers and what kind of shape it's in when it gets to you. If your pages are out of order, which has happened to a couple of readers, please let us know so we can do something about it. Leave a message on our machine (5167512600). Occasionally, a human may even pick up.

And if you have articles to send us, please do. We now pay for articles we print, so that might be incentive for some of you. Send submissions to PO Box 99, Middle Island, NY 11953.

STAFFBOX

Editor and Publisher
Eric Corley 110

Office Manager
Fran Westbrook

Cover Art
Tish Valter Koch

Writers: John Drake, Paul Estev, Dan Foley, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Bill from RNOC, David Ruderman, Mike Salerno, Silent Switchman, and the usual anonymous bunch.

Cartoonists: Dan Holder, Mike Marshall.

Editor Emeritus: TSH. (making new waves)

2600 *(ISSN 0749-3851) is published monthly by 2600 Enterprises, Inc, 7 Strong's Lane, Setauket, NY 11733. Second class postage permit pending 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—$15 individual, $40 corporate.
Overseas—$25 individual, $55 corporate.

The Ballad of

by Mike Agranoff

"The Ballad of Captain Crunch" is a fictitious story about a real person. Or, rather, a fictitious story about an imaginary person to whom I have attributed a real person's name. The real Captain Crunch is a phone freak and computer hacker, and the little anecdotal passages about how he got his name and calling himself around the world are in essence true. However, the rest of the actions and motivations concerning the main character of my story are not to be attributed to the real person, but are strictly figments of my overworked imagination. Any reading of this recitation should be prefaced with this disclaimer.

You tell of your Robin Hood legend,
The thief with the heart of pure gold,
The Lone Ranger and Tonto and Zorro and all
Of those other brave heroes of old.
You sing of Doc Holliday and old Jesse James
And the infamous wild Dalton bunch,
But alone, at the top of the list of those names
Is the man that they call...CAPTAIN CRUNCH.

Now perhaps you might laugh at this curious name,
He sounds like no prince among thieves.
And well you may ask how it is that he came
To be reckoned with such greats as these.
Well, he robbed from the rich, the richest there was,
Though he took not a penny of plunder.
And were not for him, we'd be bent 'neath a burden
We never could get out from under.

He never went armed with a pistol or sword.
He carried no longbow or quiver.
It wasn't his style to go buckle his swash,
Stop a coach and cry, "Stand and deliver!"
His weapon—an Apple computer,
His bullet, it was an I.C.
His old trusty gun was a soldering one,
His target—The Phone Company.

"Blue-boxers", they called us, and "phone freaks"
And less polite nicknames as well,
Applying the knowledge we picked up in college
In order to rip off Ma Bell.
We'd bread-board electronic circuits
Out of old Army surplus I.C.'s,
And make beepers and tooters to fool their computers
And get all our phone calls for free.

For us, it was mostly the challenge,
A game between Ma Bell and us.
They'd close down a loophole, or put up a block,
Or give us a new code to bust.
And we all got P.C.'s and modems
And broke into their internal system,
And scrambled their data and tied up their trunk lines
And did all kinds of shit that just pissed 'em!

But 'twas more than a game for the Captain.
He had a real axe to grind.
An old clerical error by Ma Bell had left him
With feelings that were less than kind.
They'd harrassed him with bills for long distance calls,
For calls that he never had made.
And 'twas only after they shut off his service
He took up the blue-boxers' trade.

He learned the trade well, and soon made his name,
When he found that the switching code locks
Could be broke with a tone from a whistle that came
In a Captain Crunch cereal box.
He would dial up an 800 number,
And before the phone rang at all,
Give the whistle a blast, dial the number he wanted,
And never get charged for the call.

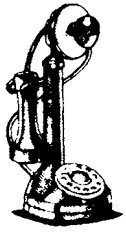
You might say that he'd found his true calling,
Discovered where his talent lay.
I remember the time that he pulled off a feat
That still stands as a legend today.
From a pay phone in Grand Central Station,
Dropped a dime, and his signal he hurled
Via satellite, cable, and microwave relay
And talked to himself round the world!

Captain Crunch

I never met him in person.
I never knew his true name.
Don't know what he looked like or where he called home,
But I counted him friend, just the same.
All I knew was his voice and his renegade soul
And his tireless quest for perfection,
And I met him along with the rest of that crew
At the North Manitoba Connection.

Now, the North Manitoba Connection
Was a central Canadian exchange,
A juncture of trunk lines from provinces north
With a side effect that was most strange:
Through a quirk in the system that Bell never planned,
(If they even knew of it at all)
Those who knew how could use the exchange
As the ultimate free conference call!

You could dial up a code any time, day or night
And converse with whoever was there.
'Twas the permanent floating blue-boxers' convention
With membership from everywhere.
There was Iggy from Fargo, and "Sparks" from Detroit,
And the Swenson boys out of St. Paul.
And we'd bullshit for hours, swap jokes, or talk shop,
Or just listen, say nothing at all.



It was sometimes so crowded, you just couldn't think.
But one night, at a quarter to three,
There were only the three of us on the exchange:
The Captain, and Lenny, and me.
Now, Lenny, he was our inside man,
An R&D tech at Ma Bell.
He had access to codes and computer net links
And hints of new products as well.

And he told us, "They've made a new breakthrough
On a miniaturized personal phone.
The bandwidth's been squeezed and the lines megaplexed
Till we each could have one of our own.
And the unit's so small, it could fit in your ear
Or be surgically placed in your head."
Said I, "I'd remove it to go on vacation!"
"That would be illegal!" he said.

A pregnant moment of silence...
Then he said, with a sputter and cough,
"George Orwell's 1984 is at hand!
How the hell could you turn the thing off?
You could never hang up, leave the phone off the hook
Or be out of the reach of Big Brother.
Except that with old Ma Bell at the controls,
It would be more like 'Big Mother'!"

"Once they convince the American public
To give the contraption a try,
You might as well take what's left of your privacy,
Smile, and kiss it goodbye!"
They'll put ads on TV, shove it down all our throats
As only the Phone Company can,
"My God!" says Lenny, "What on Earth can we do?"
Says the Captain, "I have a plan!"

"Have you ever heard of a gremlin?
That creature of legend that lurks
In the bowels of a system as complex as this
And makes sure the damn thing never works?"
"No such luck!" replied Lenny, "They've got the bugs out.
They've run all the kinks through the mill
They finished a field trial, did not see a glitch."
But the Captain said, "Oh, but they will!"

(continued on page 11)

Getting the Most Out

by The Hobbit

The axing of good ole Ma Bell has rendered wrong everything you now know about phone companies. The procedure for placing a long distance call is now above the understanding level of a good proportion of the public, and the various companies are doing very little to educate them. Thus this attempt to inform the reader what new evil lives at the other end of his pair.

In areas that are now equal access, it is possible to place a long distance call using any of the carriers who will complete it for you. You do *not* have to have previously set up an account with the carrier, as in the past. They will complete the call and pass the billing back to your local operating company (LOC), which in turn bills you for the call. So to place the call via the "alternate" carrier, you pick up and dial:

10nnn + 1 + area code + number

The nnn is magic: it allows you to select a different carrier for that call. There are a zillion little Mom-n-Pop carriers in different areas, but here are some of the major ones whose access codes should be fairly consistent.

220: Western Union— consistently bad audio 90% of the time

222: MCI— duplexey lines sometimes

288: AT&T— you know the story

333: U.S.Telecom— reasonably ok

444: Allnet— a major reseller of others' services

488: ITT— bad audio, useless for modems

777: GTE Sprint— usually good quality—rivals AT&T

When you complete a call this way, via a carrier who "doesn't know who you are", you are referred to as a "casual caller". Most of the major carriers will complete casual calls. The smaller ones usually want an access code and a pre-existing account. Note that all this is perfectly legal and nobody is going to come pound on your door and demand your firstborn for making your calls this way. The fun part starts when one considers that this two-stage billing process involves a lot of red tape and paper shuffling, and the alternate [i.e. not AT&T] carriers often have poorly designed software. This can often lead to as much as a 6-month lag time between when you make the call and when you get the bill for it. There is a chance that you won't get billed for some calls at all, especially real short ones. And if you do get billed, the rates will be reasonable. Note that if you don't have an account with a given company, you won't be able to take advantage of any bulk rates they offer for their known customers.

It is likely that for this reason, i.e. all the mess involved in getting the billing properly completed, that the local Bell companies are attempting to *suppress* knowledge of this. Notice that when you get your equal access carrier ballots, nowhere do they mention the fact that you can "tenex" dial, i.e. 10nnn, through other carriers. They want you to pick one and set it up as your 1+ carrier so you don't have to learn anything new. Now, it's already highly likely that the little carriers will fold and get sucked up by AT&T and eventually everything will work right again, but this policy is pushing the process along. The majority of people aren't going to want to deal with shopping around for carriers, are going to choose AT&T because it's what they've come to trust, and their lines are still the best quality anyway. However, the more people become casual callers, the more snarled up the billing process is going to become, and the resulting chaos will have many effects, one of which may be free calls for the customers, and the carriers and LOCs being forced to either straighten up their acts, disable casual calls and lose business, or knuckle under completely.

So where can you get more info about equal access, if not from your local company? You call 800-332-1124, which AT&T will happily complete for you, and talk to the special consumer awareness group dedicated to helping people out with equal access. They will send you, free of charge, a list of all the carriers which serve your area, with their access codes, customer service numbers, billing structure, and lots of other neat info. The LOCs will give out this number, but only under duress. They will *not* give out any information about other carriers, including what ones serve your central office, so you shouldn't even bother trying. It's apparently been made a universal company policy, which is ridiculous, but the case.

Let's get into some of the technical aspects of this. First off, you might ask, why 10nnn? Well, it could have been 11nnn too, but it wasn't. If you think about it, other numbers could be mis-parsed as the beginnings of area codes. 3-digit

# of Equal Access

carrier codes also leave plenty of room for expansion (haw!). Some of the carriers won't complete casual calls, and may even give recordings to the effect of "invalid access code". Basically when you dial this way, your central office simply passes the entire packet containing your number and the number you want to call to the carrier and lets the carrier deal with it. You'll notice that this process takes longer for some of the carriers. The carriers have differing database structures and hardware, so it takes some time to figure out if it knows who the calling number is, if bulk rates apply, and a few other things. While it's doing this search, you get silence. What's a lot of fun is that in areas that have recently gone equal access, the central offices do this exact same process for public phones. And since the carrier usually has no idea of what a public phone is, it happily completes the call for you as though you dialed it from home. It is unclear who gets the resulting bill from this, but it usually doesn't take them long to fix it. It's conceivable that the carriers can hold numbers to *not* complete calls from in their database, as well as regular customer numbers.

Some carriers also handle 0+ calls. If you dial 10nnn 0+ instead of 1+, the office will hand it off as usual, and you'll be connected to the carrier's switch, which gives you a tone. You are expected to enter your authorization code at this point, and then off the call goes. This is so you can complete equal-access style calls from friends' phones and use your own billing. It also requires that you have an account with the carrier already and an authorization code to use. Some carriers, in places where the public phone bug has been fixed, will handle 1+ calls from them this way as well. This mechanism introduces a security hole, because it's real easy to determine the length of a valid authorization code from this since something happens right after the last digit is dialed. Carriers that don't do this will sometimes tell you to dial "operator-assisted calls" by dialing 102880+ the number you want. Already they're admitting that AT&T is better than they are.

"The procedure for placing a long distance call is now above the understanding level of a good proportion of the public, and the various companies are doing very little to educate them."

(continued on page 14)

And as if this wasn't enough, carriers that do this will also usually connect you straight to the switch if you dial 10nnn#. The LOCs are finally getting around to using the # key as sort of an "end-of-dialing" feature, so you can reach the switch directly without having to dial a local number or 950-something. Being able to get to the carrier's switch is useful, because they often have special sequences you can dial there to get their customer service offices, various test tones, and other things. If you get the switch and then dial # and the tone breaks, you may have one of these. Another # should bring the tone back; if digits have already been dialed then # is a regular cancel or recall. Some carriers use * for this. Anyway, if # breaks the tone, an additional digit may start a call to an office. You can tell if it's working if # has no further effect; you'll eventually either hear ringing or nothing if that digit hasn't been defined. Many of the carriers have magic digit sequences that would otherwise look like authorization codes, but go off immediately upon being dialed and call somewhere.

Call timing and billing is a very hazy issue with the alternates, as one may see from the consumer group sheet. AT&T is still the only one that can return called-end supervision, i.e. the signal that tells your local office that the called party has picked up. The alternates, although they may be planning to install this through agreements with the LOCs and AT&T, have not done so yet, so they use timeouts to determine if billing should be started yet. These are usually the time that 8 rings takes; assuming that most people will give up after 6 or 7. So if you listen to your brother's phone ring 20 times because he went out drinking last night and is now dead to the world, you will get billed for the call whether he wakes up or not. This is sort of a cheapo compromise, but since AT&T is so reluctant to hand them supervision equipment, their hands are sort of tied. But

the telecom informer

BY DAN FOLEY

Updated Equal Access List

Once you pick an equal access long distance carrier, you aren't stuck with using just that one to make calls. By entering 10XXX (where XXX is the carrier code of your choice) you can make phone calls on other carriers. Don't be fooled into thinking that these are free though. Sometimes calls on other carriers may not catch up with you for several months. However if you try this from a hotel phone, it will never get back to you. Also, third party payphones handle these calls incorrectly, so the owner of the phone line gets the bill, not you. In response these phones are often "fixed" so that you can't make these calls.

End of Non-1+ LD Dialing

The last area of the country that did not require 1+ dialing for long distance will disappear on November 1st, 1987. A few CO's in 301, 202, and 703 still allow the old ESS programming hack which distinguished between local and long distance calls by the second digit of the exchange/area code. Every number in 202 is dialable either using 202 as the area code or instead either 703 (Northern VA) or 301 (Maryland). The calling area is second largest in the US, about 70 miles in diameter, second only to Atlanta. Any number can be dialed from any phone "locally" (i.e. without an area code or 1+). According to the North American Numbering Plan (where the acronym NPA—Numbering Plan Area, also known as area codes, came from), the second digit of an area code *has* to be either a 1 or a 0 (i.e. 212, 516, 201, 703). Central office exchange codes were not allowed to use either the 0 or 1 as the second digit (on a telephone dial neither the 0 nor the 1 has an equivalent letter combination, therefore when they named exchanges for the town or area which it covered (as in PENnsylvania-5600) none had a 0 or a 1 as the second digit. This plan worked well for years, but as loyal *2600* readers know, many downtown urban areas used up all possibly allocated three number combinations (which is a lot, about 8*8*10 = 640 exchanges handling 6,400,000 numbers (but read on before you think I'm exaggerating), as the first and second digits couldn't be 0 or 1). Code fill was nowhere near over 6 million, as often downtown business areas had old inefficient X-bar switches, and the phone company couldn't dare shut down an area for even a day to do a switchover to ESS. Also, with the proliferation of computer and data lines in the 70's along with a huge expansion in American business's bureaucracy and the growth of the skyscraper office building.... Well, you see what I'm leading up to? Yup, the telcos needed every damn exchange they could get their hands on (especially as companies liked their own Centrex or PBX exchanges). In the mid-70's (the exact date is published somewhere in the last three years of *2600*) Los Angeles (213) had the first exchanges with a 1 or a 0 as the second digit (they used Canadian area codes). As this practice spread, it became neccessary to get rid of the ESS hack which allow users to avoid the 1+ for long distance. Now even this measure is ineffectual, as was demonstrated when Los Angeles was broken into 213 and 818, and New York City into 212 and 718.

Newly Direct Dialable Countries

For those of you trying out your blue boxes or bogus cellular ROMs, AT&T announced effective March 13, 1987, that it was adding routing to even more exotic corners of the globe. Using 298 as your country code you can reach the Faeroe Islands. Greenland is now 299, Malta is 356, Micronesia is 691, and the Marshall Islands are 692. You used to be able to dial the Faeroe Islands via Denmark (1+45+42) but no longer. The Faeroe Islands, like Greenland, are a self-governing region of Denmark. Tonga (676) may also become direct dialable at this time too. Tonga was

(continued on page 22)

still more on the world of cosmos

We've run articles in the past about COSMOS, the famous program used by the phone company to control your phone line. However, we seem to have created more questions than answers in attempting to tackle the subject. Now, we approach it with more of an eye to detail. Just about everything the COSMOS expert would need to know should be here, while everything beginners need to get an idea of the capabilities of COSMOS should also be included. If, after reading this, you still have questions, write to us care of the Letters Editor. You have the right to know.

by Bill From RNOC
Legion of Doom

COSMOS is a database program used by various telephone companies to keep track of central office facilities. COSMOS gives information such as: how many cables or telephone numbers are currently available and what their status is. COSMOS is used by many departments now. It was originally for use in the frame room and loop assignment center (LAC), for keeping track of both wires and paper (orders).

When someone orders a new telephone line from the business office, the request for service is entered into a billing computer. Once the billing details are in order a service order is input into COSMOS. The fact that a service order placed in COSMOS can theoretically be completed without billing is most likely what attracts hackers the most. Keep in mind that COSMOS doesn't complete the orders, the people who use it do.

Dispelling COSMOS Myths

You cannot get from a COSMOS system in Massachusetts to one in New Jersey. Each BOC (Bell Operating Company) computer system is unrelated.

You cannnot get onto LMOS (Loop Maintenance Operation System) from COSMOS. In earlier versions there were two commands—LMOS and LMOSH which were used in transferring data tape from COSMOS to LMOS. This is no longer done.

History

Bell Labs set out to design a mechanized system which would alleviate paperwork—thus COSMOS was born in the early 70's. COSMOS is now supported by Bell Communications Research (BELLCORE). COSMOS can now run on several types of computers. The DEC PDP 11/70 and the PDP 11/45 (no longer used) run COSNIX as the operating system. On AT&T 3B20, COSMOS is running under UNIX (5.0.5). Generic 16 is the latest version. When generic 17 comes out it will only run on UNIX-based COSMOS systems. It will run on the following superminis: AT&T 3B20, the Sperry CCI, and some Pyramid supermini. Further ahead COSMOS may be run on big mainframes, but that idea is just on paper now.

If you find UNIX based COSMOS you will not be able to tell it from any other UNIX system. It does not prompt you for a wire center (WC) until you have entered a valid login and password.

```
login: rc01
password:
* = * = * = * = * = * = * = * = * = *

 Welcome to COSMOS system 3!!!

 cosmos 16.0.3    unix 5.0.5

 Data line trouble call: 611

 Data base info call: 555-1212

* = * = * = * = * = * = * = * = * = *
wc? 26

 26%      <---and you're in!
```

In this first section I am dealing with COSNIX (God rest its soul).

```
NAME: COM1
PASSWORD:
WC? 26

TT23: MUX=DJ DELAY=5 UPLOW ECHO LOGIN
********** WELCOME TO COSMOS 15.4.8.7 SYSTEM 3 **********
**********************************************************
          LAST TDAS TAPE LOADED ON 04-01-87

      ATTENION ALL FRAMES!!- .SCPA IS UP AND RUNNING.

                HAVE A NICE DAY!
**********************************************************

260
```

What does this all mean?

TTxx: is the teletype (TTY) that the user logged in on. TTY numbers range from TT01-TT96. You can also get your TTY number by using the TTY command. The system console is TT00. The options for a specific TTY are kept in a file

(continued on page 15)

The Ballad

(continued from page 5)

"Lenny, help me get into their system.
We'll show those bastards what for!
The entry code's secret, that much I know
So we'll have to go in the back door.
From the trash bin, go get the old print-outs,
The results from the latest field test.
Leave them in the phone booth on 12th Street and Main,
And I will take care of the rest!"

Then he dropped out of sight for a couple of months,
We heard nothing from Lenny as well,
Till the phone rang one night with a call from his wife
With a pretty sad story to tell.
Seems they found him one day after work in the lab
With his nose where it didn't belong,
And threatened to send him to jail if he didn't
Spill out every thing he'd done wrong.

Now Lenny was never the strongest of men,
And who knows what they threatened to do?
But they wrung out of him every secret technique,
Every blue-boxer's trick that he knew.
Then they fired his ass, left him out on the street,
Turned their energies in our direction.
And their very first act was to be to shut down
The North Manitoba Connection.

That news hit us hard. It's surprising to find
How important these little things are.
'Twas as if they had bulldozed the house you grew up in,
Or shut down your favorite bar.
And us phone freaks were hermits, for the most part,
Except within our own little clan.
And the Exchange was the bridge 'tween our personal islands,
Our one link with our fellow man.

On the evening the shutdown was scheduled,
The entire contingent was there.
We didn't talk much; there was not much to say,
Just a feeling of gloom in the air.
Then one at a time, as the lines each were cut,
One voice, then another went dead.
And more than one throat was constricted with tears
As our last goodbyes, they were said.

Then abruptly, my phone became silent,
With a silence can only be known
By the deaf, or survivors of nuclear blast,
Or a man with a dead telephone.
To the silence, I whispered, "Forever farewell!"
Though I knew that no one could have heard.
And the silence replied in a voice that I knew,
"Well, 'forever' is so strong a word!"

"Hey Captain! My God! Where are you? How you been?
And where've you been gone all this time?
And how did you manage to tap in my circuit
After they pulled out the line?"
"Better not ask how I am," he replied,
"And better not ask where I've been.
Suffice it to say that I've fixed it so that
When they locked you out, they locked me in!"

"You might say that I'm no longer a part of your world,
No longer reside on your plane,
But the trillion connections twixt billions of phones
Form a system complex as man's brain.
And now I am part of that system:
A meld of computer and mind.
You could say I'm the Phone Company's conscience,
And I'll see to it they toe the line!"

"Gotta go now, can't keep this line open much more."
And his voice faded out to a hiss,
And I sat in the dark, a dead phone in my hand,
Left alone contemplating on this:
In a way it is fitting, the way he would choose,
And things worked out just as they should.
He's gone to blue-boxers' heaven:
Tapped into the system for good!

Well, you know the rest of the story.
The facts are no longer in doubt.
Perhaps you subscribed to the personal phone
When the newfangled thing first came out.
And the thing never worked, or would scream in your ear
Or hung up in the middle of calls,
But now you all know, that was just Captain Crunch
Grabbing old Mother Bell by the balls!

(continued on page 22)

PRINTABLE LETTERS

An Envelope Please

Dear *2600*:

I don't object to the price increase. After all, it costs money to publish *2600* and your group isn't operating as a charity to phone phreaks. However, I do object to the new policy of mailing issues without envelopes. You may not consider *2600* to be an underground or illegal publication, and perhaps it isn't. But *2600* isn't exactly *Newsweek* either! I haven't seen *2600* on the magazine rack next to the Irrational Inquirer and *TV Guide* while I was waiting in the express line with my twelve items or less!

In this country we are supposed to have "Freedom of the Press," and I'm all for it. However, with the Reagan Administration era of decreased personal privacy and freedom, a *2600* subscriber can't be too careful. The postal clones have been known to report recipients of "subversive" material to the authorities for possible surveillance and harassment. I for one cannot afford to add any fodder to my FBI file. Hoover's Henchmen probably have enough material on my activities to write a short novel already! Let's minimize the amount of paperwork some pencil-pushing bureaucrat has to do by mailing *2600* in envelopes where it will be away from the prying eyes of Big Brother. I want future issues of *2600* to come to my mail drop in envelopes.

About the new format of *2600*: it looks great! Unfortunately, it doesn't fit well into a 3-ring notebook like the old format did. How about changing back to the original style? I bet it would be cheaper, too.

The article "TAP: The Legend is Dead" by Cheshire Catalyst in the January 1987 issue confirms what most of us already knew: that Cheshire is a jerk! He was literally stealing from his fellow phone phreaks for three years. It just goes to show that you can't find an honest criminal these days. What ever happened to honor among thieves?

By the way, where did you ever come up with the name Richard Cheshire? His real name is Robert "Ozzie" Osband and the "Large Manhattan Bank" that he worked for is Republic National Bank, located at 452 Fifth Avenue and 40th Street. His phone number is 212-569-5459.

Discreetly,
Bob Gamma

First of all, we never would support the notion of minimizing paperwork for bureaucrats. Think about it. If everybody who receives 2600 *had a file opened on them for that reason alone, the bureaucratic machinery would become so bogged down that it would never be able to function efficiently. And that would be in everybody's best interests as far as we're concerned.*

Seriously, reading 2600 *is nothing to worry about. You would be amazed if you saw the kinds of people and organizations that subscribe. The only people who read* 2600 *that should worry about being "watched" are those that are already being "watched". In other words,* 2600 *does not enter into it.*

Assuming "Big Brother" knows about 2600*, we really don't see what difference getting it in an envelope that has our return address on it will make. Either way, "they" know you're getting it. What we're more concerned about is whether or not it's being manhandled or delayed in the post offices. Domestic customers should receive* 2600 *no later than the 20th of the month. If this is not the case, call us so we can do something about it.*

We will continue sending your magazine in an envelope even though this costs us extra. We consider it an obligation to our subscribers for getting us this far.

And about that phone number you gave us—that's simply an answering

machine that Cheshire set up in a friend's apartment to send and receive messages. More often than not, it seems, the outgoing message has been changed remotely by outside influences. Retributive hacker justice, perhaps.

Comments...

Dear *2600*:

New format is very readable. But incompatible with old-style "3-ring binder" format. How do I add to my complete collection of back copies?

"Continued on page XX" is perhaps necessary for cheap tabloids. We all read all the mag, so you don't have to "bribe" us by putting all article beginnings up front.

Am I really the only life subscriber?

AH

We are quite aware of the incompatibility. But second-class postage requirements are such that our magazine must be 24 pages or more in order to qualify for reduced rates. We simply cannot afford 39 cents a piece, which is the first-class rate. At the same time, a 24 page issue with our old size is currently impossible. We could drill holes in the new format but then we'd have to print less on a page to accomodate the holes. Since the new format is easier to carry around, it shouldn't be hard to devise a method of filing. We'd appreciate suggestions from readers on this.

We avoid "jumps" whenever possible. But the realities of laying out a magazine sometimes make them inevitable. And, no, you're not the only lifetime subscriber. We have a few and they are all quite happy knowing that their $260 has earned them the right never to be bothered with having to renew again.

And More Comments...

Dear *2600*:

I have a few comments on your new format. First, I miss the large format. Its large pages were easier to read, and the page-numbering made referencing simple. I also miss the loose-leaf holes. As stated in your first issue (I have them all), *2600* should be filed for reference purposes. The new format makes this very difficult.

I think I see your intentions: you want *2600* to become a widely distributed and accepted magazine, maybe even sold at newstands or bookstores (where a flashy cover is important for impulse sales). I myself, as a subscriber and supporter of *2600*, would *not* like this method of distribution to be undertaken. For one, it's expensive. A fancy three-color cover does nothing for me except use up my subscription dollars which could be better spent printing more information. I just don't feel *2600* has mass-market appeal.

To sum up my opinions, *bring back the old format!* Just add new pages and columns as necessary, and keep the halftones.

P.S. You wasted four valuable pages by printing cellular telephone frequencies that can be derived from this simple formula:

FREQUENCY=869.97+(CHANNEL*.03) where: CHANNEL=1 TO 666

CHANNEL=(FREQUENCY-869.97)/.03

Frequency=870 to 889.95 Mhz

Bernie S.

Correction: we only wasted three valuable pages. And, while some considered that a waste, others were happy with it because, for the first time, they could actually see what the frequencies were instead of having to calculate them. After all, what would they do with the calculation? Probably, print out a list. Seems like we've saved them a couple of steps, doesn't it?

As far as distribution at newstands is concerned, 2600 does have a future here. We have experimented with a few and had positive results. We find this to be a great way to attract new

(continued on page 1

Equalling the Access (continued from page 7)

notice that it's likely that you won't get billed for a real short call that is answered quickly, either. With the advent of 9600 baud voice-grade modems, this could have some interesting applications as far as message passing is concemed, and avoids pissing off operators by trying to yell through non-accepted collect calls or long lists of what person-to-person name meant what. But in general, you should keep your own records of what call and what carrier and if it completed or not, so you won't get erroneously billed by a silly timeout.

Carriers often use their own switching equipment; they also often lease lines from AT&T Long Lines for their own use. Allnet, for example, leases equipment and time from other carriers at bulk rates and resells the service to the customer. So if you use Allnet, you can never tell whose equipment you're really talking on, because it's sort of like roulette between satellite, microwave, or landline and who owns it. Some of this latter-generation switching equipment is warmed-over AT&T stuff from a few years ago, and therefore may be employing good old single-frequency trunks, i.e. 2600 Hz will disconnect them. In the early days of carriers before equal access, 2600 would often reset the local switch and return its dialtone. This is less common these days but there's a lot of equipment still out there that responds to it.

When you select your default carrier, there is another valid option that isn't on the ballot. It is called "no-pick", and is not exactly what it sounds like. If you simply don't pick one or return the ballot, you get tossed into a lottery and you will wind up with any random carrier as your default on 1+ dialing. You still won't get bulk rates from this carrier unless you call them up and create an account [or you may get a packet of info from them in the mail anyway, because if they got selected for you they will probably want you to sign up]. However, no-pick is the condition where you *do not* have a default carrier, so if you pick up and dial 1 + area + number the call will not complete. This is great for confusing people who attempt to make long distance calls on your phone and don't know about tenex dialing. Probably your best bet as far as saving money goes is to sign up with *all* the carriers, and examine their billing structures carefully. You can then choose the one that's cheapest for a given call at a given time. You may need a computer to do this, however. It is surprising that nobody has yet tried to market a program that will do this for you.

Post-parse, or 10nnn0+ dialing, is not the only security hole that carriers have to deal with. There are often magic sequences that, when dialed after a trial authorization code, will inform the caller if the code was valid or not without having to dial an entire number. These usually take the form of invalid called area codes, like 111 or 0nn or *nn. Most of the carriers have fixed the problem in which an invalid code plus some sequence would return silence and allow recall, and a valid one would error out. This allowed valid codes to be picked out very quickly. Longer authorization codes and improvements in the software have largely eliminated this as a major problem, but it took a few years for them to get the idea. Note that abuse of other peoples' authorization codes *is* illegal and they will probably come after people who do it. However, it is often interesting to play around with a carrier you are interested in purchasing service from, and see if you can break their security easily. If you can, then it's clear that someone else can, and this carrier is going to have a lot of problems with fraud. Someone may even find your code and then you'll have to deal with bogus billing. So if you find some algorithm which allows you to come up with a 6 to 8 digit valid code, one thing you might do is call the carrier and tell them about it. They'll thank you in the long run and might even offer you a job, a side benefit of which may be unlimited free calling via their equipment.

cosmos: the universe unfolds

(continued from page 10)

called /ETC/LINES.

MUX=: PDP 11/70's can have different types of multiplexers. DJ is a DJ11 mux. These are asynchronous, 16 line multiplexers. DZ is a DZ11; these are less expensive than the DJ11. A DZ11 is an asynchronous 8 or 16 line mux. MUX=DK indicates DATAKIT VCS (Virtual Circuit System). A DK allows users to select which system they wish to enter. An 11/70 hooked up to a DATAKIT usually has 60 TTY's (as opposed to 96).

DELAY=: This word specifies the number of nulls (control-@) to be sent before each line. The nulls sent are equal to the DELAY number. Many users log on to COSMOS with printing terminals. These printers cannot always print as fast as they can receive. Nulls will give the printers more time to print without slowing down CRTs. Too many nulls slow down 300 baud so they are kept at a moderate level.

UPLOW: COSNIX uses only upper case. UPLOW converts lower case and echos it in UPPERCASE. This is achieved by running a program called /BIN/LCASE when a user logs on.

ECHO: Indicates that the computer will echo back (full duplex).

LOGIN: Indicates that you just logged on.

COSNIX, like UNIX, has an /ETC/PASSWD (password) file. This is similar to the UNIX PASSWD file but has some differences. Here is a sample /ETC/PASSWORD file:

```
ROOT:ME2IDORF:0:::1:/:/USR/COSMOS
BIN:ME2IDORF:1::Y:1:/BIN:/USR/COSMOS
COM1:EPOHA3DU:2::Y:1:/USR/TMP:/USR/COSMOS:/USR/PREOP:/USR/SO:/USR/MMC
COM2:EPOHA3DU:3::Y:2:/USR/TMP:/USR/COSMOS:/USR/PREOP:/USR/SO:/USR/MMC
PA01:0062DAER:4::Y:3:/USR/TMP:/USR/COSMOS:/USR/SO
PA02:KSLH1NPA:5::Y:3:/USR/TMP:/USR/COSMOS:/USR/SO
NA01:4D17YT21:6::Y:3:/USR/TMP:/USR/COSMOS:/USR/SO
IN01:DROLOOHS:7::Y:3:/USR/TMP:/USR/COSMOS:/USR/SO
RC01:DAED7IBF:8::Y:3:/USR/TMP:/USR/COSMOS:/USR/SO
FM01:LOD1HNJ7:9::Y:3:/USR/TMP:/USR/COSMOS:/USR/SO
SS01:PSOSDEF9:10::Y:3:/USR/TMP:/USR/COSMOS:/USR/SO
```

The fields of a COSNIX /ETC/PASSWD are as follows. The fields are separated by colons ':' in the password file. The fields are as follows: 1) username, 2) encrypted password, 3) user number, 4) description fields (unused), 5) dialup user (Y for yes, nothing for no), 6) user group (1=full access, 2=shell user, restricted access), 7) home directory, 8) path, 9) path....

The COM accounts are used by the mini-computer maintenance center (MMC) or the COSMOS database manager (DBM). 0:1 is the only user who can execute the change of password command. As in UNIX, /ETC/PASSWD can be left unprotected but is almost never left that way.

COSNIX has another file called /ETC/LINES. This file lists the TTY numbers and which users can access them. It also specifies duplex, baud rate, and privileges (in some cases).

```
1-2,USERS=ROOT;BIN;COM1,ECHO,UPLOW,DELAY=5,MESSAGE
3-9,USERS=PA*;NA*;RC*;COM2,ECHO,UPLOW,DELAY=5
10-22,USERS=PA*;NA*;FM*;RC*;SS*;IN*;COM*,UPLOW,DELAY=10
23-60,USERS=FM*;SS*;IN*,ECHO,UPLOW,DELAY=5
```

The first field is the TTY number. USERS= indicates which users access which TTYs. If a user has an asterisk after the group name then it allows all users. If a line doesn't have the word ECHO there, then it's for half duplex users only. MESSAGE will write a message to TT00 (the system console) stating that someone just logged on with privs. If you login with privs on a MESSAGE tty your prompt will be an asterisk. If the /ETC/LINES file is changed, a security feature of COSNIX will pick it up.

```
COSNIX prompts  WC% = average user
                WC0 = super user, user group 1 in /ETC/PASSWD
                WC* = super user MESSAGE TTY in /ETC/LINES
```

The /ETC/MATRIX.S file says which users can access which COSMOS commands. COSMOS commands are kept in the /USR/COSMOS directory.

```
/  PERMIT MATRIX    04-01-84
/  UPDATED FOR 15.4.8. ON 11-25-85
/* COSMOS USER-CATEGORY-TRANSACTION PERMISSION FILE

/* LIST OF FAMILY NAMES AND CATEGORY ASSOCIATED WITH EACH
NAMES:
/ SYSTEM ADMINISTRATOR
<COM>; 01.;
/ LOOP ASSIGNMENT CENTER (LAC)
<PA>; 02.;
/ FRAME ROOM
<FM>; 03.;
/ RECENT CHANGE MEMORY ADM. CENTER (RC MAC)
<RC>; 04.;
/ INFORMATIONAL USERS
<IN>; 05.;
/ SPECIAL SERVICES
<SS>; 06.;
NAMESEND:
ALLTRAN:   / =0 MEANS USE MATRIX TO DETERMINE TRANS. PERMISSI
       0  / =1 MEANS ALL TRANSACTIONS ARE PERMITTED.

CATEGORY:
       0
/* TRANSACTION VERSUS CATEGORY PERMIT MATRIX
TRANX:

/*   1 2 3 4 5 6 >
<ACE 1 1 0 0 0 0 >
<ADT 0 0 0 0 0 0 >
<AIT 1 0 0 0 0 0 >
<ALF 1 0 0 0 0 0 >
<ALI 1 0 0 0 0 0 >
```

what cosmos can do to you

```
<ALK 1 0 0 0 0 0 >
<ALP 1 0 0 0 0 0 >
<ARB 1 1 1 1 1 1 >
<AUD 1 0 0 0 0 0 >
<AZC 1 1 1 0 1 0 >
<BAI 1 1 1 0 1 0 >
<CAY 1 1 1 0 0 0 >
<CCA 1 1 1 1 0 0 >
.
.
.
<WCC 1 1 1 1 1 1 >
```

The /ETC/MATRIX.S file gives the different user group numbers, then makes a table cross-referencing them with command names. A 1 means that family can use the command and a 0 means they can't.

Prefixs and brief descriptions:

AO: Associated order: When creating a service order (ORD), the option AO can be used. This indicates that there is another ORD pertinent to the one being worked with. The two orders should be completed together.

BL: Bridge Lifter: These are used with telephone answering services (TAS). The TAS has an extension of the customer's line. A BL allows one location, the customer's house, to have priority. If the TAS is on the customer's line, and the customer picks up, he will have priority and the TAS will be disconnected.

BTN: Billing Telephone Number: This indicates that one line's calls get placed on the bill of another line.

CCF: Custom Calling Features. COSMOS has an option which can define the features (three way, call waiting, etc.) on a line. These features would be, for the most part, listed by three characters. This option can only be used with electronic or digital offices.

```
. CUSTOM CALLING FEATURES TABLE:

INDIVIDUAL CCF'S
****************
SAM             SAMPLE FEATURE
  1ES=1/1AESS       EF2=2/2BESS       3ES=3ESS
  DMC=DMS 100                         5ES=5ESS
```

[SAM is the feature identifier code in COSMOS. The codes following the switch names (1ES, DMC, 5ES, etc.) would be the feature identifier code on the different electronic/digital switches.]

```
ESM             CALL FORWARD POTS
  1ES=ESM           EF2=ESM           3ES=ESM
  DMC=CFW                             5ES=/CFV

ESX             CALL WAITING POTS
  1ES=ESX           EF2=ESX           3ES=ESX
  DMC=CWT                             5ES=/CWT
```

```
ESC             3 WAY CALLING POTS
  1ES=ESC           EF2=ESC           3ES=ESC
  DMC=3WC                             5ES=/MW3WC

ESL             SPEED CALLING 8
  1ES=ESL           EF2=ESL           3ES=ESL
  DMC=SC1                             5ES=/IDSC1C

ESF             SPEED CALLING 30
  1ES=ESF           EF2=ESF           3ES=ESF
  DMC=SC2                             5ES=/IDSC2C

EAN             CONFERENCE CALLING CENTREX
  1ES=EAN,E2H       EF2=EAN           3ES=
  DMC=CNF                             5ES=/MW6WC
```

CP: Cable Pair: A CP is the wire which goes from the central office (CO) to the customer's premises.

CS: Class of Service: RES, BUS, PBX, DTF (Dial Tone First coin line). The CS is a general service category. It varies from place to place.

DD: Due Date: A DD is simply the date a specific ORD should be completed by.

FDD: Frame Due Date: This is the date when all work on the Main Distributing Frame (MDF) should be completed. It is usually a day or two before the DD. This will ensure that the line is working, before a lineman goes to the customer's premises.

FEA: Features: These are line features common to all types of switching equipment. [1] **T**ouch tone/**R**otary. [2] **S**leeve lead/**N**o sleeve. A sleeve is part of a subscriber trunk. A grounded sleeve indicates the line is busy. Customers who own fancy equipment such as a PBX will have sleeve lead. This means the sleeve will be run into their location. [3] **E**ssential service/**N**on-essential. Essential service means that the customer is on a priority service list, in case of emergency. If the switch were to break (electro-mechanical) or crash (electronic), the customer's line would be one of the first restored. Essential service also indicates a good chance to get a toll call through when lines are tied up (i.e. flood, hurricane, bombing of small Middle Eastern country). Usually doctors, coin phones, and government officials have essential service. [4] **G**round start/**L**oop start. A normal line is loop start meaning when you pick up the phone you get a dial tone. If a line is ground start you must touch the tip (lead) to ground to get a dial tone. Ground start lines are mostly used by PBX customers.

HF: Hunt From: This indicates that when the line specified after the HF is busy calls will hunt to the TN in question.

—and what you can do to it

HT: Hunt to: This indicates that when the line is busy calls will hunt to the given TN.

LOC: This is the location of either the CP or OE on the MDF.

OC: Order Class: An OC represents special treatment for an ORD. I am not fully familiar with the different types. OC HOT indicates that the ORD is on a priority completion list and should be done right away. This is normally used when a customer has a service failure.

OE: Office Equipment: An OE is the physical piece of equipment that a line takes up in the switch. In electronic offices there is a line card with memory which holds the attributes of the line. In electro-mechanical offices an OE is a small network of electronic components: changes are hard wired and not kept in memory.

ORD: Order Number: An ORD is the service order's name. It is indefinitive but follows a certain standard. It can be any group of characters (up to 25), but is usually the OT followed by 6 numbers (ORD OT123456).

OT: Order Type: An OT signifies what a specific ORD does, whether it's a new line or just a change made to an old one.

PIC: Primary Independent Carrier: This option, while hardly used, will display the customer's equal access choice by its 3 digit code. Some systems use the alpha code, while most use the numeric.

NOTE: This is not a complete list of carriers but covers most of the big ones. This list serves a double purpose as the PIC codes are the same as equal access 10XXX codes.

PIC	Alpha	Company Name
001	RTT	Republic Telecom
007	TMC	TMC
009	MCR	?????????
011	MTD	Metromedia Long Distance
040	???	Teledial America
053	ANN	American Network
066	???	MAI/Lexitel
080	???	Autel
084	LDS	?????????
211	RTC	RCI
220	WUT	Western Union Long Distance
221	TSR	Telsavers
222	MCI	MCI/AMEX/Sears Long Distance
223	TDI	TDI Inc.
224	ACT	???????????
224	AME	???????????
228	ATX	AT&T
234	ACC	ACC
245	TDT	Taconic Telephone
258	???	Metronet
272	BPA	Bell of PA
286	???	Clark Long Distance
288	ATT	AT&T
322	ASH	American Sharecom
333	UST	US Telecom(now US SPRINT network 1)
345	NCF	??????????
362	ELC	Electronic Office Center
421	CLK	Coalink
432	LGT	Lightel (Doesn't want name being given out.)
442	FNE	?????????
444	ALN	Allnet/ALC
452	VNS	Virtual Network Services
456	ACC	Argo Communications
488	ITT	ITT Longer Distance Service
497	ECA	Econo-call
539	LDX	LDX
555	TLP	TeleSphere
652	NJB	New Jersey Bell
654	CBD	Cincinnati Bell Long Distance
698	NYT	New York Telephone
776	???	Liberty Telephone (950-1776 cute)
777	GSP	GTE SPRINT (now US SPRINT network 2)
800	RCA	RCA/Satelco
826	TLM	TEL MAN
833	BTI	Business Telecom
835	TLC	TeleConnect
850	TKC	TollKall
852	TSI	Telecom Systems
888	SBS	SBS Skyline (now MCI)
963	TNX	???????????
999	SNC	Starnet Corporation

PL: Private Line: A PL is a special circuit set up between two CO's. It can be a foreign exchange (FX), or WATS, or just any type of long distance connection. A PL name can be up to 25 characters and has little other information about it kept in COSMOS. PL information is usually kept in TIRKS (Trunk Integrated Record Keeping System).

SE: Special Equipment: SE is used when a circuit, usually a PL, requires something which cannot be achieved with an OE. When you look up a line owned by TELCO (Telephone Company) instead of a cable pair, it will have house cable. It will look like this:

```
SE HSE.CBL   ST WK    DATE 04-10-87
```

TN: Telephone Number: This is a telephone number, plain and simple.

TT: Telephone number Type: This is not rigid. When a COSMOS database is set up, different TN's are asssigned TT's. They do not have to be stuck to, but they are a good idea (organization, how novel).

USG: USOC (Universal Service Order Code): This is the COSMOS equivalent of an LCC. For example: 1FR, 2FR, 4FR are 1, 2, and 4 party line flat rate. 1MR and 1MB are measured residence and measured business. DTF and DFA are dialtone first coin. 1OF is an official TELCO line.

Essentially, a phone line is comprised of a CP--the wire which runs to the customer

(continued on page 20)

(continued from page 13)

readers who would otherwise never know of our existence. We in turn will provide them with knowledge that they never thought was obtainable. This does not mean we're "selling out" or trying to get mass-market appeal. If you go to a halfway decent newstand, you'll see quite a few other magazines reaching out in the same way.

An Experience to Share

Dear *2600*:

One bright day last March, a week after my 16th birthday, I came home to discover that the cops had raided my room and taken everything—computer, printer, modem, monitor, 350 disks, but left the Apple IIc power pack. Among those 300 disks were about 20 phreak/hack disks, 300 pirated programs, and a number of personal disks. MCI had caught me hacking out codes and put a Dialed Number Recorder on my line. They had followed all my calls for 1½ months.

My first meetings with probation and lawyers scared me to death. I was informally threatened with going to juve, having to pay immense fines, never getting any of my stuff back, etc. The next 2 months of waiting for my trial were hell. I was originally charged with 9 counts of various crimes including phone fraud, accessing of MCI's computer, and annoying phone calls (exchange hacking).

As it turned out I used a county lawyer and ended up paying nothing for his services. I got off on most of the counts and had to pay a fine of $479.32, $29 of which were phone bills and the rest were "service charges" of having to switch the 22 codes I used. I also had to serve 80 hours of community service and remain on probation until these items were done.

I got all of my computer stuff back minus 11 disks of phreak/hack stuff (they missed quite a few). I did pay the fine which was a hell of a lot less than what it should have been. I actually completed about 15 hours of community service but my probation officer was easily deceived.

I just got off probation last week and all and all I've got to say it was well worth it. I wrote to give you my account of being caught and what the end resolution was (not very harsh). I do hope that none of you have to go through what I did in those first 2 months.

The Sultan

Getting caught at something illegal is never "worth it" unless it's something you really believe in or something you can erase later. And if you brag about this to lots of people, you'll probably find yourself reliving history. Keep us posted. We care.

Words of Agreement

Dear *2600*:

Just a quick note to tell you I agree with your new format (except it's too bad it doesn't come three-hole punched). Keep up the good work—getting my first issue of *2600* (December 1986) was like a breath of fresh, ionized air.

DE

Words of Caution

Dear *2600*:

The mailman brought me your "surprise" and I found, after quickly reading cover-to-cover, that I felt as though your excitement/pride was something that I also felt a part of. Thanks for being there...thanks for moving ahead...thanks for all your efforts to allow us all to enjoy the ride.

One worry did creep into my mind: will *2600* somehow move into a mainstream approach to its product/-subject/readers. It is my hope that you remain true to your present direction. Tell it like it really is...like it can be (given the very creative people out there). "Rub the lamp...call out the

(continued on page 23)

2600 marketplace

I'D LIKE TO TRADE PC software with ANYONE having an IBM PC or compatible. At present my PC library approximates 110 products including the latest games, diagnostic programs, business software, utilities, and various word processing and other application software. Readers can contact me by writing: Software, PO Box 73, Uniondale, NY 11553.

INSTRUCTIONS FOR THE CONSTRUCTION AND OPERATION OF THE BLUE BOX WANTED! I am a beginning phone enthusiast and would greatly appreciate it if someone could help me in designing a blue box. Of course, as you might have guessed it, this is for "informative" purposes only! Send your replies to Mr. Oscar Statuto, 224A Washington St. #9, Lynn, MA 01902.

WANTED: A decent modem program for use on a Zenith Z-100 running MS-DOS. Contact Manny @ 2600, (516) 751-2600 or PO Box 752, Middle Island, NY 11953.

DOCUMENTATION on electronic & digital PBX's and switching systems. Willing to trade/purchase. Also looking for Bell System Practices and other such paraphernalia. Write to Bill, c/o 2600, PO Box 752B, Middle Island, NY 11953.

CELLULAR TELEPHONE INFORMATION WANTED. I will pay a modest fee for info which has not yet been published in 2600. Please describe the type of info that you have and name your price. Mr. B., P.O. Box 2895, Brooklyn, NY 11202.

MANUALS OR INSTRUCTIONS NEEDED for two modems labeled Dataphone Channel Interface. One has label on the outside that says: 44A2 Series 1, Data Mounting, SD-1D247-01-J23 and the other says: 44A2 DATA MTG, SD-1D247-01-J23, SERIES 1 83 MG 12. The boards on the inside are labeled: DAS 829B-L1A, SERIES 4, 81MG3 and DAS 829BL1A, SERIES 5, 84 MG 04. Send info to: P.O. Box 50346, Raleigh, NC 27650.

PRIVATE INVESTIGATOR wants to hear from 2600 readers who have electronic equipment he can buy cheap! Gaslamp Private Eye is into Electronic Countermeasures/TSCM in the trade parlance. 425 "F" Street, San Diego, CA 92101. (619) 239-6991.

TAP BACK ISSUES—complete collection, vol. 1-83 plus supplemental reports and schematics. Approx. 400 pages of quality copies sent via UPS or US Mail. $100 includes delivery. Send cash, check or MO (payable to PEI). Cash sent same day, others allow 4 weeks, to: Pete G., Post Office Box 463, Mt. Laurel, NJ 08054

HEY YOU! This is the chance you've been waiting for! A rather new service of *2600* Magazine. Got something to sell? Looking for something to buy? Or trade? This is the place! And it's free to subscribers! Just send us whatever you want to say (without making it too long) and we'll print it! Only people please, no businesses!
Deadline for April issue: 4/5/87.

(continued from page 17)

everything you always wanted

premises. The TN is the network address dialable from anywhere, and the OE is the equipment which makes it all work.

Modifiers

CP: BL, LOC
TN: BTN, HF, HT, TT
OE: CCF, CS, FEA, PIC, US
ORD: AO, DD, FDD, OC, OT

CP status:

WK: Working pair, in use.

SF: Spare, unused.

RS: Reserved for future assignment.

UK: Unknown. This is rarely used, and shows sloppy work on the part of TELCO.

D1-9: Defective cable:

D1: short circuit

D2: ground ring side

D3: ground tip side

D4: cross battery

D5: open ring side (ring side not connected)

D6: open tip side

D7: open both sides

D8: ground both sides

D9: unbalanced voltage

PC: Pending connect. The CP is being added to a circuit.

PD: Pending disconnect. The CP is being removed from a circuit.

TN status:

WK: Working, in use.

OF: Official TELCO line.

TS: Test line. Used on loop, terminations, recordings....

UNQ: Unique. Used for special numbers, such as NNX-0000.

SF: Spare, willing, and ready (for assignment).

NP: Nonpublished number, used when customer changes old number due to a problem such as crank calls. The NP informs people looking up the line to not disclose information.

AV: Same as SF. Seems rather silly to me.

UK: Unknown, someone spilled coffee on the paper work.

DO: Disconnected number. Instead of a recording there will be an operator to announce a change in service.

DM: Disconnected machine (recorded) intercept. "The number you have reached has been disconnected..."

CO: Changed number, operator intercept.

CM: Changed number, machine intercept.

PC: Pending connect, the TN is being added to a circuit.

PD: Pending disconnect, the TN is being removed from a circuit.

(In all cases if a facility (TN, OE, CP) is either PC or PD, it will have a regular status (WK, SF, DM, etc.) also.)

An OE status is the same as both a CP or a TN status code.

OT—order types:

NC: New Connect. A new circuit is being built.

CD: Complete Disconnect. An existing circuit is being removed.

CH: Change. An existing circuit is being changed (new TN, different FEA, etc.).

F and T: From and To. These are AO. I'm not too familiar with them.

SS and RS: Suspension/Restoral of Service. These are used when bills are left unpaid!

TT—telephone number types:

B: Business line. Usually thousand, or hundred group numbers (i.e. NNX-2000, NNX-2600, etc.).

C: Coin line, usually in the 9XXX range.

D: Official TELCO line. Usually NNX-99XX or NNX-00XX numbers.

T: Test line. Usually NNX-99XX or NNX-00XX numbers.

G: Good. This as far as I can tell is assigned to numbers which can be both residence or business lines. The numbers are usually catchy—NNX-1222, NNX-1212, NNX-1234, etc.

X: Other, basically your run of the mill number (i.e. NNX-9089 or NNX-7689, etc.).

Q: Centrex numbers. Usually a hundred group range (i.e. NNX-1000 to NNX-1099).

To get a listing of orders in COSMOS you can use the SOL command. On the Hunt line of the SOL it says OT NC. This will only print out an ORD if its type is a new connect. You can specify OT, OC, DD, FDD, and ORD in an SOL.

```
260 SOL
N OT NC
.

                    APR 01, 1984   12:23:00 PM                    PAGE 1

                    COSMOS SERVICE ORDER LISTING

                         INPUT OPTIONS:
                         OT NC
WIRE CENTER : 26


ORDER NUMBER      DD OT DUE_DATE CXT_ID      CABLE_PAIRS ST OC  HD/JR AI
NC260011-A           NC 04-07-84 511-4050    115-0507 FC
NC660112             NC 04-09-84 511-4010    113-2091 AC        DD
NC666312             NC 04-09-84 511-7462    113-0214 AC
NC663066             NC 04-10-84 511-0012    115-3117 AC
NC663231             NC 04-10-84 511-5643    113-0331 AC
NC831023-A           NC 04-11-84 5 'C INTERRUPT

260
```

to know about cosmos

The column called CKT-ID has the telephone numbers. The column headed AI has the ORD writer's initials. I'm not that familiar with ORD status codes, but there is an easier way to find out what's happening. You can use the INQ or the SOI command to list out an order.

```
260 SOI
H ORD #C666312
-*

                APR 01, 1984    12:24:56 PM

            SERVICE ORDER ASSIGNMENT INQUIRY

ORD #C666312                OT(NC)   ST(AC- )   FACS(YES)
   DD(04-06-84)  FDD(04-05-84)  EST(03-30:16)
   MOF WORK REQ(YES)  MOF COMPL(NO)  LAC COMPL(NO)  RCP(NO)
CP  113-0214
    ST SF  PC     FS WK   DATE 09-24-83
    LOC PF11013
OE  005-5253
    ST SF  PC     FS WK   DATE 01-12-84    CS BUS      UB IND      FEA TNEL
    LOC PF11013
TN  511-7462
    ST SF  PC     FS WK   DATE 03-03-84    TYPE I  HF TN 511-7400
    BTN 511-7400


** SOI COMPLETED
260
```

FACS(YES) states that the order was implemented in conjunction with FACS (Facility Assignment and Control System). FACS is a network of computers including COSMOS, WM (work manager), LFACS, and others.

MOF WORK REQ(YES)—this means that frame work is necessary.

MOF COMPL(NO)—the frame has not completed the appropriate work.

LAC COMPL(NO)—the loop assignment center has not completed its work.

RCP(NO) has to do with forms being sent to the proper places. I'm not quite sure how that works.

EST(03-30:16) is the time the order was input to COSMOS: March 30th at 4pm.

LOC is the location at the MDF (frame) where the CP and OE meet.

Cosmos Fun!

```
260 WHO (cr)
ROOT     TT00 CN
INO1     TT20 EM
COM1     TT23 26
RC01     TT51 CD
MA01     TT57 26

260 WHAT (cr)
COSMIX 15.4.8.2 OPERATING SYSTEM
SUPPLEMENTAL RELEASE VERSION
NOVEMBER 21, 1985
COSMOS GENERIC 15.4.8.11
MARCH 16, 1986
```

```
260 WHERE (cr)
2600 ENTERPRISES
PO BOX 752
MIDDLE IS., NY 11953-0752
COMPUTER NO. 2

260 TTY (cr)
TT23

260
```

An example of the three W's of COSMOS. WHO tells you which users are logged into which TTY and which WC. WHAT gives you the COSMOS version and WHERE gives you the location of the computer. TTY tells you what TTY you are on.

Bell Labs humor: This is a little joke (very little) in COSMOS.

```
260 ARG (cr)
 ^C   AARRRGGHH!! PROCESS KILLED
26#
```

Using the LTN (List Telephone Number) command you can scan for test lines. On the hunt line the NNX or 511 is specified and a status of test is specified. This makes it easy to 'scan' for test lines.

```
260 LTN (cr)
H NNX 511/STT TS
-*

                APR 01, 1984    12:29:16 AM                    PAGE  1

          LTN - LIST OF TELEPHONE NUMBERS IN STATUS TS


                          NNX 511

TELEPHONE PRTN PEND ASSIGN  AY        STATUS                  RELEASE  SEQ
 NUMBER   STAT STAT  STAT  TYPE TYPE   DATE   REMARKS          DATE    NUM

511-0557   TS                  I   06-27-83 SYNCH-OPR-TST
511-1360   TS                  I   05-10-83 SHORTED-TERM.
511-1369   TS                  I   05-11-83 900-OHMS
511-1370   TS                  I   05-11-83 OPEN-TERM.
511-2199   TS                  I   05-11-83 PERM.-BUSY
511-2300   TS                  D   05-20-83 MILLIMATT
511-2301   TS                  T   05-20-83 PORT-0-TST
511-2302   TS                  T   05-20-83 PORT-1-TST
511-6611   TS                  0   05-12-83 MONSANTO
511-8150   TS                  I   05-23-83 TRL-INTC
511-8151   TS                  I   05-23-83 CUS-CLR-ERR
511-8152   TS                  I   05-23-83 PS-MON-CH-OPER
511-8153   TS                  I   05-23-83 PS-CH-OPER
511-8154   TS                  I   05-23-83 OVERFLOW-RON
511-8155   TS                  0   05-23-83 INITL-CH-TST
511-8156   TS                  I   05-23-83 1PLUS-DIAL-ERR
511-8157   TS                  I   05-23-83 VERIFY-REQ.
511-8158   TS                  I   05-23-83 OPER-CH
511-8476   TS                  I   02-13-84
511-8903   TS                  I   02-08-84 BTDTEST
511-8999   TS                  0   04-08-83 IFR-TEST
511-9497   TS                  I   04-08-83
511-9499   TS              ^C INTERRUPT

260
```

The REMARKS column holds information which can be helpful when 'scanning'.

To get a list of WC's, you can type WCFLDS (W. C. Fields).

cosmos

```
26# WCFLDS <cr>
ACTIVE WC'S ARE:
26
CN
DB
EM
PS

26#
```

The last command is one which you should never execute, unless you have access to the tape drives. Nevertheless, it makes a good finish to the article.

```
26# LOG <cr>
  0, 1, 2 or E ENTER? E <cr>

 ** LOG TAPE ERROR--- END PRESENT AND START NEW TAPE

;LOGIN:
```

Telecom Informer *(continued from page 8)*

assigned 676 last year, but implementation was delayed. Translations for local central offices around the country to accept 676 as Tonga haven't been rescinded even yet.

Captain Crunch

(continued from page 11)

It's been a few years since they closed the Exchange,
When the Captain set off on his own.
We've since seen divestiture, Sprint, MCI,
And the ten dollar Japanese phone.
When I ring up his phone, a recorded voice says,
"This number's no longer in service."
But I know he keeps vigil, and I know he keeps watch,
And I know he still makes Ma Bell nervous.

And now sometimes when listening to answering machines,
Or sometimes when I'm on hold,
A voice will come through to me, faint, but distinct,
A voice I remember of old.
And you'd think it was leak-through from some other line,
But I know that he's talking to me.
It's old Captain Crunch keeping watch on Ma Bell,
The soul of the Phone Company.

Mike Agranoff is a folk singer from Boonton, NJ. He also plays concertina, banjo, recorder, as well as many other instruments. His *Ballad of Jake and 10-Ton Molly* has achieved nationwide acclaim through the performances of Bill Staines. He's a board member and past president of the Folk Project, and manager for that organization's coffeehouse, The Minstrel Show.

His collection, *Jake, the Captain, and Other Heroes*, is available for $6.00 postage paid. Write to Mike Agranoff, RD 4 Box 45 Oak Hills, Boonton, NJ 07005.

* * * * * *

As many of you know by now, the real Captain Crunch, John Draper, was arrested in late December for something that had absolutely nothing to do with phones.

According to police, Draper was helping to manufacture fake Bay Area Rapid Transit (BART) cards in San Francisco. These are the cards you insert into machines that read a magnetic strip and either demand money, let you pass, or give back money. Washington DC also has this kind of a system.

Draper, who was arrested with two others, has pleaded not guilty to charges of forgery, conspiracy, and computer fraud. He's free on $11,500 bail.

According to the *San Francisco Bay Guardian*, it's become a sort of sport to try and outwit the BART system. In fact, several colleges in California had contests, the results of which were widely circulated among crackers. This caused BART to change the system once and now it appears they'll have to do it again.

We're happy that Captain Crunch cracked another system, if that's in fact what he did. We hope, however, that he wasn't selling forgeries to the general public, as he's being accused. There's nothing clever or ingenious about the latter and, if convicted of this, it would relegate the Captain to the status of a common thief, not to mention the probable prison term involved.

We don't want to see hackers and phone phreaks going to jail for being stupid and/or greedy. That's a waste of a real talent.

By the way, we're told that Pacific Bell has entered the case because Draper allegedly used "sophisticated electronic equipment" to gain free access to the long distance telephone network. That's a pretty fancy way to describe a touch tone phone, isn't it?

(continued from page 18)

magic forces...let Uncle Sam figure out how to control what comes forth...let *2600* readers enjoy the thrill and excitement of fresh ideas and the raw power that comes from new information in the hands of young minds without restrictions."

Ben Harroll
San Diego

Now why didn't we say that?

A Response

Dear *2600*:

Your new format for *2600* looks good. Thanks for the extra effort to improve it, and keep up the good work. Also, thanks for the fine TAP article by Cheshire Cat.

We must respond to Arab 149's complaint that we charge too much ($2 each) for copies of back issues of TAP, and that we are ripping-off the work of others by doing so.

Consider:

(1) No issue of TAP was copyrighted. When you don't copyright your work, it falls into the public domain and anyone can copy and distribute it. And it implies that you either don't care or actually want this to happen.

(2) We advertised in TAP and contributed articles to it.

(3) We highly recommended TAP in several of our publications. We, as well as dozens of Consumertronic's customers were ripped-off of subscription fees to TAP. And we lost substantial credibility and business because of this. A few people even falsely accused us of being in cahoots with TAP.

(4) Before selling copies of TAP, we wrote TAP as to our intentions, and we notified mutual acquaintances of TAP staffers. And we openly advertised the resale of TAP back issues. At no time did we ever receive any objection from any former TAP staffer for doing this. And no staffer, to our knowledge, competed with us to sell TAP back issues.

(5) Arab 149 does not understand the economies of numbers. Orders for TAP back issues average about two issues per order. There's a lot more work involved per issue in making one copy compared to making 100 copies. More work means more money! Also, we charge $160 for copies of all 91 back issues. Also, TAP issues are difficult to copy. Constant changes in copier contrast and reduction must be made as TAP issues have many different formats and print densities. It's a tedious job! $2 per issue is reasonable!

(6) Consumertronics is a profit-making business. We support ourselves and children with it. Please realize that but for Consumertronics, *2600*, and a few others, where would you acquire this invaluable and unique information during a time of increasing government and big business rip-offs and oppression? The personal freedom situation is much worse today than it was in the sixties when a lot more people had the balls to protest and fight wrongdoing. We need your support to continue! Think about that the next time you feel that you are paying too much for information that was difficult, costly and risky to acquire, and risky to publish!

John J. Williams
Consumertronics
2011 Crescent Dr.
Alamogordo, NM 88310

More on ICN

Dear *2600*:

Here is something about ICN that I found in the February '87 issue of Consumer Reports:

"In Wisconsin, the attorney general recently obtained a temporary injunction against a second flat-rate company, Independent Communications Network. Among other things, ICN must now disclose that fewer than 5 percent of its customers' calls go through."

I also have one question—does anyone know ANI for Montana?

Jim A.
Montana

CONTENTS

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.

WARNING:
MISSING LABEL