2600 July, 1984

Published monthly by 2600 ENTERPRISES, INC. | An unincorporated association. Subscription: $10 annually, $9 semiannually, and $1 per back copy. Write to 2600, Box 752, Middle Island, NY 11953.

FIRST ISSUE VOLUME ONE, NUMBER SEVEN

"LOOK OUT, HE'S GOT A COMPUTER!"

Fear of computers is one thing. Almost everyone has experienced this to some extent, though some of course are able to handle it far better than others. But *misunderstanding* of computers is a great deal more damaging and far less recognized among the mainstream.

What's the difference? The two are definitely related, there's no denying that. But they are far from identical. One of the most outstanding differences lies in the fact that people who claim to be "afraid" of computers (whether it's because of their efficiency, rapid growth, or whatever) tend to keep away from the things. But people who misunderstand computers are the ones who are running and regulating them.

Last month it was reported that Tom Tolmpidis, who operates a computer bulletin board system from his home in the Los Angeles area, had his equipment seized by the Los Angeles Police Department. Why? Somebody somewhere had called up his system and left an AT&T credit card number posted. Pacific Telephone found out and decided to flex its muscles. Officials involved in the case insist that the system operator be held responsible but it's impossible to ascertain *why*. The man who approved the search warrant, Superior Court Judge Robert Fratianne, was quoted in *InfoWorld* as saying, "As far as I can see, for someone to commit a computer crime, they have to have the knowledge, the equipment, and the access to an illegal [bulletin] board." Does anyone know what he's talking about? What in the world is an *illegal* board? What kind of equipment is he talking about? The only equipment here is a home computer! In another article, one of the officials claims that he knows all about this kind of thing, because he saw *War Games*, the film where a kid tries to start a nuclear war. Perhaps he didn't see the same film as the rest of the world, but in any event, seeing *War Games*, whether you understand it or not, doesn't make you an automatic expert on anything having to do with computers! This is what is known as aggressive ignorance.

Another fun thing that happened last month was the TRW escapade. The nation was shocked to find out that the TRW computer, which houses credit information on a *large* number of people, *might* have been broken into. Nobody knew what had even happened! Did someone raid the system and destroy or change info? Did the feds bust another BBS for posting "illegal" info? Were real criminals involved this time? Did a large bill get sent to an innocent corporation? According to all of the articles that have been written, not one of the above happened, but they all *could* have happened. So where is the story?! Are they saying that the worst thing that happened here was the posting of this nifty information somewhere? Well, that's not even interesting since any employee that uses the system could tell someone else about it at any moment.

Again, what we are seeing here is a failure to appreciate the full implications of such a thing. There is a story in this whole TRW thing. But it's not in the possibility that some hacker somewhere figured out a password. The story lies in the existence of the TRW database itself. Why was this completely downplayed? Because an article about kids breaking into a computer makes for good, sensationalist reading. It doesn't matter if most of the information is totally wrong, the people will read it. Nobody wants to read about how we're losing whatever freedom we have left, not to a machine, but to the people running the machine. It's depressing to hear about your entire life story being written to disk somewhere and to know that there's not a thing you can do about it. But, like it or not, this is *exactly* what's happening.

It's quite possible that TRW has a file on you that can be checked and appended by people all over the place. It's also entirely possible that some of that information is wrong. And it's a fact that TRW itself claims no responsibility for the accuracy of this info. But even if all of the information *is* right, how do you feel about being categorized?

On the back pages of our issue this month, we've devoted some space to the way TRW operates and the information that can be found. We didn't print this so that everybody could figure out a way to break into their system, although we'll certainly be accused of this by our critics. We're publishing these facts so that as many people as possible can become aware of the wide availability of increasingly personal tidbits and how this can affect us for the rest of our lives. We're doing this so that people can realize how easy it is for items to be altered and for assumptions to be made by people reading this data. Look at the sample printout and see if its thoroughness surprises you. Try to imagine how thorough it could become in ten years with improvements in technology and continued erosions of personal freedom. The FBI recently came very close to expanding its files on criminals. They wanted to include "known associates of criminals." Next would have come "known associates of known associates," etc. They lost the battle for the moment, but you can count on seeing another drive for this increased surveillance real soon.

What many are not realizing is that this constitutes true "misuse" of computers. What kind of a society are we heading towards that wants to keep close personal data on *everybody*? Regardless of whether or not one is on the right side of the law, nobody wants everything about them to be known. We all have our secrets and more systems like TRW will make those secrets increasingly hard to keep. But according to today's papers, the biggest problem with computers are the hackers.

People who do little more than type some numbers onto a terminal and do a little bit of thinking are referred to alternately as computer geniuses and computer bandits by the media. And nearly every story written about such things is full of astronomical lapses, misinformation, corporate sympathy, and the obligatory Donn Parker quotes. *The Washington Post* recently did a three-part story on "computer crime" which said absolutely nothing new. It could have been manufactured by a computer program!

Meanwhile, legislators are tripping over themselves trying to get laws passed to *control* these computer people before they take over the world. The intensity with which the FBI has chased hackers in the past year or so indicates the power they think those with computers either have or are capable of achieving. And most of this fuss is being made over people simply *accessing* other systems. What in the world is going to be the reaction when people finally start to *use* the computers, to calculate and design?

A new bill has been proposed to outlaw computer crime. Isn't that wonderful? Do you know what they consider a computer crime? Personal use of a computer in the workplace. This means that if an office worker were to open a file and write a note to himself reminding him to stop at the store later on, he'd be committing a felony. Plans are also in the works for bills that would add penalties to crimes that were committed with the help of computers. In other words, stealing is stealing, but stealing with a computer is stealing and a half.

The hysteria continues. The United States government is doing everything in its power to prevent the Soviets from obtaining computers that are practically a dime a dozen here. What good could this possibly achieve in the long run? And why pick on the computer? It's not a weapon in itself, but merely a tool. A *vital* tool, yes, but still tool.

It's clear that computer people are in for an era of harassment from the authorities, who haven't been this riled up since Prohibition. And everyone else will be getting it from the computer illiterates, who insist on tracking everything that moves. We can survive by staying awake. But we'd better start working on it.

MCI MAIL: The Adventure Continues

You really have to hand it to those folks over at MCI. First they tackle Ma Bell and now they're going after the U.S. Postal Service! MCI Mail's slogan, "The Nation's New Postal System," is printed on every bright orange envelope that they send through, you guessed it, U.S. Mail.

On this system a user is assigned a "mailbox" that he can use to send and receive mail. Sending is done either electronically, that is, to other people with MCI mailboxes or through the post office, which covers everybody else in the world. The first type of letter will cost you $1 for the first three pages while the second type is double the cost. It's also possible to send an overnight letter ($6) or a four-hour letter ($25) to some places.

The purpose of MCI Mail is to stimulate the use of electronic mail by making it more accessible to the average person. For that we must give them credit—anybody can get an account on this system! There is no start-up fee and no monthly fee of any kind. To get an account, all you have to do is call them—either by voice or data. If you call by data (see page 5 of April issue of *2600* for numbers), you'll have to enter REGISTER as the username and REGISTER as the password. The rest is self-explanatory. After a couple of weeks, you'll get in the mail (regular mail, that is) a big orange envelope that has, among other things, your password. With this info, you're now free to log onto the system, look for people you know, send and retrieve messages, read all of their help files, or even hop onto the Dow Jones News Service (watch it though—*that* can get pretty expensive!)

The system is set up on a network of Vaxes throughout the country. They've been operating since September 1983 and claim to have over 100,000 subscribers. Many of these are actually subscribers to the Dow Jones service, who are automatically given MCI Mail accounts whether they want them or not.

While the rates aren't overly expensive, they're certainly not cheap. Mailing regular letters is much cheaper and often just as fast since not every MCI Mail user checks their mailbox every day. Apart from that, though, there are many problems with the system as it stands now. For one thing, it can take forever getting on it, particularly through the 800 numbers. When you finally do get a carrier, you should get a message like this after hitting two returns:

Port 20.
Please enter your user name:

Enter the username you selected and the password they assigned you. It should say, "Connection initiated...Opened." From that point on, you're in.

But the system will often appear to be bogged down. Often you have to hit twenty returns instead of two. Sometimes the system won't let you in because all connections are "busy". Other times it will just drop the carrier. Real mailboxes don't do that.

Another thing that will drive you crazy are the menus. *Every* time you enter a command, you get a whole new menu to choose from. If you're at 300 baud, this can get pretty annoying, especially if you know what all the options are. There are two ways around this: get the advanced version, which allows you to enter multi-word commands and even store some files, at a cost of $10 per month, or simply hit a control O.

One part of the system that works fast and is very convenient is the user info. As soon as you type the command CREATE to begin writing a letter, you'll be asked who you want to send it to. Enter either the person's last name, first initial and last name, or username (which is usually one of the first two, but which can be almost anything the user desires). Immediately, you'll get a list of everyone with that name, as well as their city and state, which often don't fit properly on the line. There are no reports of any wildcards that allow you to see *everybody* at once. (The closest thing is *R, which will show all of the usernames that you're sending to.) It's also impossible for a user not to be seen if you get his name or alias right. It's a good free information retrieval system. But there's more.

MCI Mail can also be used as a free word processor of sorts. The system will allow you to enter a letter, or for that matter, a manuscript. You can then hang up and do other things, come back within 24 hours, and your words will still be there. You can conceivably list them out using your own printer on a fresh sheet of paper and send it through the mail all by yourself, thus sparing MCI Mail's laser printer the trouble. You could also share your account with somebody else and constantly leave unsent drafts for each other. Again, they have to be retrieved within 24 hours.

Yet another way of getting "free" service from these people is to obtain many different accounts. There doesn't seem to be any kind of a limit on this and since each account comes with $2 of free messages, a few accounts can get you quite a bit of free service. And, of course, there's no charge for *receiving* messages on any of these accounts.

2600 has learned of several penetrations onto MCI Mail by hackers. This isn't really surprising considering: (a) there are multiple usernames, i.e. John Smith's username would always default to JSMITH, which means that several passwords can work for one username; (b) all passwords seem to follow a similar pattern—8 characters with the odd-numbered characters always being consonants and the even-numbered ones always being vowels—any true hacker would obtain several accounts and look for any correspondence between the random password and the account number everyone is assigned; (c) MCI Mail doesn't hang up after repeated tries—the only thing that will make it disconnect intentionally is inactivity on your part.

But by far the biggest blunder that MCI Mail has made is not found on the system. It lies in their bills. *There is no carry-over from month to month!* If you get billed for $8 one month and you don't pay it, then proceed to use the system for $3 more the next month, your next bill will only show the $3! The $8 has vanished! (This is by far the dumbest mistake we have *ever* reported in these pages.)

You'll find quite a few unanswered questions in your travels through MCI Mail, which you can try to solve by reading the HELP files or by sending a *free* message to MCIHELP. It usually takes them a couple of days to respond to you instantly, however.

There are some software lapses as well. The system seems to be patterned largely after GTE Telemail, but it never really reaches that level of clarity. A small example can be seen in the scan tables, which have a heading of From, Subject, Size, etc. On outbound messages, the name of the person you're sending *to* appears under the *From* heading! Pretty silly.

MCI Mail shows every indication of overspending with a passion. Free messages, free accounts, sloppy programming, toll-free dialups, single sheets of paper (like their bills) sent in huge envelopes, etc. Either they're very optimistic out there or they're very naive.

(MCI Mail can be reached at 8004246677.)

Look Out For Sidney!

Combined News Sources

The city of New York has come up with a new way to fight parking scofflaws. It's called SIDNEY—Summons Issuing Device for NEw York. It's a handheld computer terminal that will be able to get information about license plate numbers that are "suspected" of being attached to scofflaws.

The device weighs less than five pounds and looks rather like a calculator. It would ask whoever was operating it to enter the color, make, model, registration expiration, location, time, and nature of violation. SIDNEY would then print out a waterproof parking ticket and at the same time check its 10,000-plate memory to see if the license plate belonged to a scofflaw or a stolen car. An appropriate message would then be flashed on the screen. Details of each ticket issued would be stored in the device and entered automatically into the main computer system each day.

There hasn't been much talk circulating about what will happen when these things get stolen and fake tickets are handed out by the thousands. It is expected that these creatures will be turned loose into the hands of meter-maids within two years. The contract for producing SIDNEY has tentatively been awarded to Citisource of New Jersey.

Bell to AT&T: Get Lost!

Associated Press

One of the so-called "Baby Bells" is displaying its independence from its former parent—AT&T. Southwestern Bell says it's chosen GTE Sprint to provide long-distance telephone service for its Houston operation.

By using GTE Sprint instead of AT&T, Southwestern Bell figures to save about fifty thousand dollars. Long distance service from Houston currently costs the former Bell system unit about $300,000 a year.

GTE Sprint will replace AT&T in Houston in mid-August.

Five Arrested in Phone Fraud

The New York Times

Five Manhattan residents were arrested last month on charges of defrauding the New York Telephone Company by making more than 1,500 illegal telephone calls, mostly to the Dominican Republic, in a three-day period.

The Manhattan District Attorney's office said the suspects used "blue boxes" to make the calls. The five were charged with possession of burglary tools and theft of services. One was also charged with selling a stolen credit card number to an undercover investigator and using such numbers to make calls for other people. He could get four years for his trouble.

Supposedly, the suspects were offering neighbors low-cost long distance calls, however they frequently charged more than the cost of legitimate calls!

An Official Crackdown on Hackers

Combined News Sources

According to Rep. William Hughes (D-N.J.), computer crime is increasing by leaps and bounds. Speaking on the House floor, Hughes said, "It's time we recognized that computer 'hackers' who intrude into data banks are not just mischievous kids looking for fun. They're engaging in illegal activities which pose potentially serious threats to our society."

He urged quick passage of the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, being sponsored by him and eight other House members, including Democrats and Republicans.

The House Judiciary Committee took a step towards making it a crime for hackers to break into systems such as TRW by adopting an amendment by Rep. Dan Glickman (D-Kan.). His proposal would make it a misdemeanor to raid computer files containing private credit histories or banking information.

A subcommittee staff lawyer said the bill would close loopholes in existing federal and state laws by making it a felony offense to access a computer without authorization and with intent to defraud, if that act enables the perpetrator to obtain anything worth at least $5,000 over a one-year period or any classified government information.

The bill is expected to come before the full House either late this month or in early August.

Pay Telephones Deregulated

2600 News Service

On June 15, the FCC decided to allow just about anybody to get involved in the pay phone business. Up until now, pay phones have been provided by whichever local company serves the area. But with this new ruling, all kinds of new companies will be seen. In fact, some phones may even have different prices! And, of course, it's to be expected that each of these new types of phones will have their own quirks and bugs. Look for Matrix, Tonka, and Paytel phones in the near future.

Of course, there will be disadvantages. Some phones will only be able to dial locally. Others won't be able to reach 911 or information. Many will probably be rotary and most will certainly break down more frequently. Still, diversity is what makes this entire field so interesting.

"You Must First Dial a One..."

Associated Press

As of July 1st, 3 million customers in New Jersey had to start dialing a one before area codes when calling long distance. This leaves 202 and 516 as the last remaining areas in the country that don't have to do this.

Company officials say the new system was introduced to provide 152 more exchanges to meet increasing customer demand. Under the new system, New Jersey Bell will begin using certain area codes as telephone exchanges. They will avoid using area codes of neighboring states to prevent mass confusion.

Information News

Combined News Sources

Starting this month, MCI will connect subscribers to long distance information just like AT&T does. And, like AT&T, MCI will offer two free information calls per month, provided their service is used for at least two long distance calls in that same month. After that, they will charge for a call to information, just like AT&T does! So what's the difference? In the price, of course. AT&T charges a hefty fifty cents for each call to directory assistance, while MCI will be under-selling them with an affordable 45¢. Good old capitalism.

In another development, a computer program to help find a telephone number without complete information from the caller has been patented by Richard H. Boivie for Bell Labs. In cases where the caller can give the information operator the name of the person being sought, but is unsure about the spelling, the computer will trace alternative spellings. It will also sort through different addresses for the most likely candidates.

INTRODUCING THE CLEAR BOX!

A new device has just been invented. It's called the "clear box". It can be used throughout Canada and through rural United States.

This interesting gadget works on "post-pay" payphones, in other words, those phones that don't require payment until after the connection has been established. You pick up the phone, get a dial tone, dial your number, and then put in your coins after the person answers. If you don't deposit money, you can't speak to the person at the other end, because your mouthpiece is cut off—but not your earpiece. (Yes, you can make free calls to the weather, etc. from such phones.)

In order to bypass this, all one has to do is visit a nearby electronics store, get a 4-transistor amplifier and a telephone suction cup induction pick-up. The induction pick-up would be hooked up as it normally would to record a conversation, except that it would be plugged into the *output* of the amplifier and a microphone would be hooked to the input. So when the party answers, the caller could speak through the little microphone instead. His voice would then go through the amplifier, out the induction coil, and into the back of the receiver where it would then be broadcast through the phone lines and the other party would be able to hear the caller. The clear box thus "clears" up the problem of not being heard.

The line will not cut off after a certain amount of time—it will wait forever for the coins to drop in.

Many independents are moving towards this kind of stupid payphone system. For one thing, it's a cheap way of getting DTF (dial tone first) service. It doesn't require any special equipment. That type of payphone will work on any kind of a phone line. Normally a payphone line is different, but this is just a regular phone line and it's set up so that the payphone does all of the charging, not the CO. With the recent deregulation of payphones, this kind of a system could become very popular.

LETTERS FROM OUR READERS

6/14/84

Dear *2600*:

A few exchanges in my vicinity have recently upgraded their switching equipment. On 11/5/83, 914-268 switched from a SxS to a Northern Telecom DMS100. 914-634 & 638 also switched from a No. 5 Crossbar to a DMS100 on 6/9/84.

Through trashing, 99XX scanning, and "social engineering," I have found out the following: The suffix -9901 is a "verification" recording. In 268: 9903, 9906, 9909, 9911, 9912, & 9913 are all various recordings.

Another neat function on DMS100 is that you can hear the MF tones after most calls. NYTelco calls this the sound of their new system helping to serve you better.

Also, these CO's are under NYTelco jurisdiction. Yet, they bought from Northern Telecom DMS100 instead of a "nice" ESS system from Western Electric. Could this be the break-up at work?

This equipment offers ESS functions such as call waiting, call forwarding, dial-tone-first fortresses, etc. My question is: What type of toll-fraud equipment is standard or optional for the DMS100? Does it record everything like a pen register? Etc...

Curious

Dear Curious:

First off, our compliments on your ability to notice the changes that most people miss. As far as your 9901 discovery, many exchanges in your area have been known to do that. If you dial XXX-9901, you'll hear a computer read the exchange and area code. It doesn't really serve much of a purpose. But interesting things can always be found in the 99XX area, if your company uses it.

Concerning the DMS100, it is the break-up of the Bell System to an extent. New York Telephone has been buying equipment from Northern Telecom for some time now. But since the divestiture, they've become a little more flagrant about it. You'll see quite a bit more experimentation with products from other suppliers in the near future. The DMS100 is a very good switch, but it's got certain drawbacks as far as phone phreaking is concerned. It does have certain "devices". These don't work *exactly* like a pen register, but they wind up having the same effect. What is done is this: if you happen to send a 2600 Hertz tone down the line, DMS100 will make a computer record of whatever you did in the surrounding time. They automatically investigate your line if this is detected more than an undetermined amount of times. This is where the pen register comes in. The system is already equipped to handle a pen register through a special box in the exchange that's set up entirely for that purpose. This box ties into their automatic surveillance equipment. So it's kind of a two step process, but the DMS100 makes it much easier.

So far, we haven't been able to find any advantages (or bugs) in a DMS100. We will continue to look, though. Regarding the MF tones, they're simply not being filtered as they are in most places. The GTD#5 (made by GTE) and the DMS100 both, as a rule, only filter about ten percent of the MF tones. They also don't filter out rotary outpulses, whenever they exist. Perhaps it's a way of cutting corners.

DMS100, as you know, sounds just like ESS. About the only way you can tell if you've dialed into one is if you hear absolutely no clicks or pops when the party answers, as you do with ESS, crossbar, and step. Instead you hear a real faint, mild tick. When dialing out on one, you won't hear any clicks either.

Dear *2600*:

I hear you people are keen on answering people's questions, so answer me this: What ever happened to that operator who was so damn nasty that she refused to call that ambulance for this guy's dying mother just because he used a couple of cuz words on the telephone? By the way, the lady died a horrible violent death, I think. (I think the operator didn't die yet.) Oh yea, I also think that there was some sorta lawsuit against the nasty-oppy or the telco or someone.

RC

Dear RC:

The incident you're referring to took place a few months ago. It happened in Dallas, Texas and it concerned a man who was trying to get an ambulance for his mother-in-law who was having a massive heart attack. Not only did the operator refuse to send an ambulance until the woman herself got on the phone, but her supervisor *also* got on the line and said something to the effect of, "Sir, if you don't quit cussing out the operator, I'm going to have to hang up on you."

The operator was fired and the supervisor demoted. But both are currently claiming that they were only following orders. The city of Dallas allegedly said that at all costs an ambulance shouldn't be sent out unless it was an extremely life threatening situation. Anonymous people have even come forward and claimed that bonuses were offered to those who sent the least amount of ambulances out!

We should say that this doesn't involve the phone company, since it wasn't their operators who handled this call. Any lawsuits would be against the city of Dallas, in all likelihood. It's also interesting to note that there is no 911 service in Dallas. Residents there dial 744-4444 instead. Perhaps an advanced 911 service might cut back on the fake calls they're supposedly plagued with since such systems immediately trace back the number calling and do an instant CNA on it.

(Write to 2600, Box 752, Middle Island, NY 11953 or MCI Mail ID: 2600.)

TRW Information Services is America's largest credit reporting institute, containing the credit histories of over 90 million Americans online.

Recently it was reported that a password belonging to Sears, Roebuck, & Co. was stolen. TRW and the media are currently circulating several conflicting reports about the use of the account. Some reports insist that the account was never used illegitimately. Others say that 'criminals' used the account to pillage credit card numbers to illegally buy goods and services while knowing the account limit. Another account of the incident(s) says it was merely hackers exploring a very interesting system. It seems hard to believe that hackers managed to infiltrate TRW, since the system is basically user spiteful, but they seem to have pulled it off.

Once the subscriber initiates a connection with one of the many dial-ups, located in most major cities, the system will identify itself with TRW. It will then wait for the subscriber to send an appropriate answerback (such as a control-G). Once this has been done, the system will say CIRCUIT BUILDING IN PROGRESS along with a few numbers. After this, it clears the screen (Ctrl-L) followed by a control-Q. Once the control-Q is sent, the system is ready to accept the subscriber's request. The subscriber must first type a 4 character preamble which identifies the geographical area of the subscriber's account. For example:

TCA1 - for certain California & vicinity subscribers
TCA2 - a second TRW system in California
TNJ1 - their New Jersey database
TGA1 - their Georgia database

The subscriber then types a carriage return (followed by an optional 3 line feeds). On the next line, he must type his 3 character option. Most requests use the RTS option. OPx, RTx, and a few others exist. Some of these, such as RTA, return you with an error saying that this option is used for credit bureau collection activity only. TRW will accept an A, C, or S as the third character.

After the option (RTS), a space must be skipped, and then a 7 digit subscriber code is typed in. The first two digits represent the region in which the subscriber is located and the subscriber's industry, respectively.

Table I (first digit)	Table II (second digit)
1 - TRW Eastern Region	0 - Public Record
2 - TRW Midwestern Region	1 - Bank
3 - TRW Western Region	2 - Bank Credit Card
4 - Inquiries from Broker Customers	3 - Retail
5 - ?	4 - Credit Card
6 - Other credit reporting agencies within Eastern Region & Commercial Credit Subscribers	5 - Loan Finance
	6 - Sales Finance
	7 - Credit Union
7 - Others within Western Region	8 - Savings & Loan
8 - Others within Western Region	9 - Service & Professional

Using the tables above, it is evident that the stolen Sears Password from Sacramento must begin with a 33, identifying it as from the Western Region and as being a retail store.

Once the subscriber enters his 7 digit subscriber code which is printed along on the reports, he then appends a 3-4 character password immediately after it. (In the Sears example, the whole thing was: 3319122NXK. This code has allegedly been floating around hacker circles for at least two years!) Following this, he must type a space and then the full last name of the person he wants a report on. This is followed by another space and the full first name. After this comes yet another space.

Now the subscriber has 3 optional parameters. He can just type 3 periods after the first name and space or he can fill them in. The first period can be replaced by the person's middle initial, the second by the spouse's first initial, and the third by an S or a J which indicates Senior and Junior respectively.

The last of the three parameters is followed by a comma. This is immediately followed by the house number and a space. After the space, he then places the *first* letter of the street name. For example, he would type M for Main Street, a # for a P.O. box, or 3 for 32nd Street. This single character is then followed by the 5 digit zip code (mandatory) and a final comma. After the zip, he would hit carriage return and an optional line feed. (There are some special conditions which can apply to the house number—if an institution such as a school, motel, or hospital is given as the main address, 33333 would be used as the house number. When an address is General Delivery, 44444 would be the house number and G would be the street name. Others: U.S. Air Force, 55555 A; U.S. Army, 66666 A; U.S. Coast Guard, 77777 C; U.S. Marines, 88888 M; U.S. Navy 99999 N.)

Assuming the subscriber is calling from a California business and he is requesting a report on Winston Smith at 3 Main Street, Anytown, CA 90003 he would type the following after the control-Q:

TCA2 (This identifies the subscriber as being from CA)
RTS 33xxxxxABC SMITH WINSTON ..., 3 M 90003,
In this case, the subscriber password was ABC and the account number was represented by 33xxxxx.

At this stage, he can request the report printout by typing a terminating control-S or he can tell the computer some information that it will then record into the account. This is known as using the second line, which is entirely optional. The first option that can be specified here is a previous address. This can be done by typing P- followed by the house number, a space, the first letter of the street, another space, and the full zip. For example, if Mr. Smith previously lived at 2600 Elm Street in New York City, the subscriber would type the following: P-2600 E 10001. He can then type a comma after this and move onto another option. If Mr. Smith had another previous address, the subscriber can enter it in the same fashion as above (after the comma) if he omits the P and the dash. This is followed by a comma also. He can then enter in Mr. Smith's Social Security number in the format of S-1234567890. If this is followed by a comma, he can then enter A-age or Y-year of birth (4 digits, e.g., 1984). The subscriber can next enter in information telling how much money Mr. Smith has requested and/or on what type of account. This is done by typing T- followed by a two digit account type, a 3 digit terms, and a 3 digit amount code. For instance, for a credit card account (which happens to be #18), with a limit of $100 (001), which being financed for 24 (024) months, he would type: T-1802400. This information will show up as an inquiry under the subscriber's name on Mr. Smith's account.

There is one final option on line 2 which prints a heading at the top of the page (TRW supplies pre-printed forms with "nice" columns). If the subscriber cannot afford to buy their paper, he would probably type H-Y to get the heading. The last option on line 2 is followed by a comma, carriage return, and an optional line feed. For example:

TCA2
RTS 33xxxxxABC SMITH WINSTON ..., 3 M 90003,
P-2600 E 10001,1313 M 58102,S-1234567890,Y-1984,T-18024001,
This can then be finally entered by typing a control-S.

But wait! That's not all. The subscriber has one more option. He can specify the person's *employer*. Let's suppose that Mr. Smith works for NYTelco Security at 1095 Avenue of the Americas in New York City. The subscriber would then type:

E-NYTELCO SECURITY/1095 AVENUE OF THE AMER/ NEW YORK 10036

After this he would enter the familiar carriage return and optional line feed. (TRW emphasizes to their subscribers that this area is for the name and address of the employment only, not occupation or source of income. "Do not use terms such as 'housewife,' 'retired,' 'welfare' or 'unemployed' which could be considered damaging to the applicant," a special warning reads.) Since this is the last bit of information that the subscriber can enter, he is now forced to type the inevitable control-S.

The first line of the actual printout sends the page number, the date, the time, the port number, and the H/V (?). It will then print the person's address and their employer. After this it should print the person's actual credit history. Each individu account entry takes up 2 lines. In the first line, the accou profile, subscriber's name and TRW account number, their association code, and the individual's account number with the subscriber are listed. The A on the left is the account profile. A means that the subscriber (SAKS FIFTH, as an example) transmitted this information automatically from their computer (as opposed to an M, which means that the subscriber manually

TRW: Big Business is Watching You

pr[illegible]d forms with the info). The position of the A (or M) indicates a positive, non-rated, or negative rating (P/N) of the account. In this example, the A is under the P, therefore it reflects positively upon the account. The person has an account with Saks Fifth Avenue. Saks' subscriber number on TRW is 1347515. The person's account number with Saks is 26000000.

On the second line of each entry, the account status, date (last) reported, the date the account was opened, the type of account, the credit limit, current balance, and a credit profile are listed. For example, on the second line of the Saks entry, CURR ACCT indicates that it is a currently active revolving (REV) charge (CHG) account that was opened in October 1980. The account has a $6700 credit limit and as of April 5, 1984, the person had a $55 balance on the account. The C's and dashes indicate how the person pays the account. In March (one month prior to the balance data of 4-84), the account was paid on time. In February, two months prior to the balance date, the account was also paid on time. In January (3), the account was thirty days past due (1=30, 2=60, 3=90, etc.). In December, the account was not reported by Saks as indicated by a dash. In October, the account was sixty days past due. Court judgments, tax liens, and other interesting facts are also recorded.

The person may also have a 100 word or less statement in the file explaining certain entries in their account. (There is also another TRW service for business reports (similar to Dunn & Bradstreet) which has an entirely different set of subscriber codes and passwords, as well as access procedure.)

TRW doesn't like to be held up for anyone. Therefore, if the subscriber vegetates for more than a few seconds (i.e., he is[illegible]er sending nor receiving anything), TRW will abruptly s[illegible]RVICE INTERRUPTED; PLEASE REDIAL (EM) as it logs him off. Incidentally, any information that the subscriber types on lines 2 or 3 (i.e. age, social security number, employer, etc.) is automatically recorded on that person's file. Any previous information on the option is discarded (in most cases).

Technically, if a hacker hacked out an account belonging to a supreme court or other such institution, he could use the T-option to hack out the code for JUDGMENTS, TAX LIENS, and other neat things. He would then be able to modify anyone's account to report them bankrupt or that a judgment was handed down.

Hacking passwords is still reported to be very easy. Assuming that someone is trying to guess a password to a 3xxxxxx account, the following could be done:

TCAI
RTS 3000000AAA (return, control-S)
and the system responds with:
**** xx ** INVALID SECURITY PASSWORD**
and the hacker types:
TCAI
RTS 3000000AAB (return, control-S)
and the system responds with:
**** xx ** FORMAT ERROR**

The hacker has correctly guessed the password—it accepted the password but didn't find a name field. Since account numbers are very easy to get ahold of, the password is the only real challenge. That, and the fact that the system operates on half duplex, even parity, 7 bits, and 2 stop bits, which might catch a few by surprise.

All accounts can do reports on anyone in the United States th[illegible]s a file. For example, if a California account requested d[illegible]n a person in New York, the system would simply switch over to its New Jersey database to accomodate the request. A few states though, such as Tennessee, have government control over credit information. Thus, people from that state cannot be found on TRW. Can *you* be?

```
TCA2
RTS 1234567ABC SMITH WINSTON ....3 N 90003,
P-2680 E 19801,1313 N 58102,S-1234567890,Y-1984,T-1802A001,
E-NYTELCO SECURITY/1095 AVENUE OF THE AMER/NEW YORK 10036

  1  04-03-84  15:25:02   AA23  A55  SMITH                TCA1
     WINSTON SMITH                    4-84 NYTELCO SECURITY
     3 MAIN ST                              1095 AVENUE OF THE AMER
     LOS ANGELES CA 90003                   NEW YORK 10036


P / N SUBSCRIBER NAME        SUBR # ASSN          ACCOUNT #          MONTHS PRIOR
      STATUS     DATE   DATE TYPE  TERM ANT  BAL  BALANCE  AMOUNT  TO BAL DATE
      COMMENT    REPRT  OPEN                     DATE     PAST DUE 1234567890123

------FILE IDENT:  SS# IS 1234567890,SPOUSE INIT IS J,YOB IS 1984

  A   B OF A                  3101344 5                 1234260000000
      TOO NEW RT  4-84  1-00  AUT   48 $6000 $600   4-10-84
A     S P N B                3110260 0                 260000000
      CURR ACCT   10-Y  10-Y  CHG   REV  $100
A     CROCKER BANK             3120354 1                 2600000000000
      CURR ACCT   4-84  5-77  C/C   REV $2000 $1219  4-17-84
A     SEARS                    3319842 0                 2600000000000
      CURR ACCT   3-79  10-Y  ISC    14  $100    $0                    CCCCCCCCCCC
A     BROADWAY                 3370300 1                 26000000000000
      CURR ACCT   4-84  3-83  CHG   REV $1000    $0  4-02-84           -CCCCCCCC
A     MAY CO                   3370510 1                 2600000000
      CURR ACCT   4-84  8-81  CHG   REV  -$100   $28  4-16-84           CCCCC
A     BULLOCKS                 3371400 1                 26000000000
      CURR ACCT   3-84  1-77  CHG   REV  $300   $133  3-09-84
A     J W ROBINSONS            3371559 0                 26000000
      CURR ACCT   4-84  7-82  CHG   REV  $400    $0   3-09-84           CCCCC
A     CARTE BLANCHE            3425200 1                 2600000000
      CURR ACCT   12-83 5-81  CRC     1 $1400 $1484 12-31-83           CCCCCC

------ATTN: FILE VARIATION: ZIP IS 90004/OTHER FILE IDENT: SS# IS 123333333,
            MID INIT IS Z,SPOUSE INIT IS S

A     CITIBANK                 1391556 1                 2600000
      CURR ACCT   2-83  6-78  CHG   REV  -$100    $0  2-31-83           CCC--CCC-CC
A     SAKS FIFTH               1347515 1                 26000000
      CURR ACCT   4-84  10-80 CHG   REV  $6700   $55  4-05-84           CC1-C2CC3CC-
A     NORDSTROM                3390286 1                 26000000
      CURR ACCT   8-83  8-83  CHG   REV  UNKN    $0  12-15-83           CCCCC
A     G E C C                  3600711 4                 260000000000000
      CURR ACCT   12-83 9-83  CHG   REV $1500 $1275  12-15-83
A     CRSI/DESMOND             1391554 1                 260000000000000
      CURR ACCT   8-82  UNKN  CHG   REV  -$100    $0                    CCC-CCCCCCC
A     T W A                    2455618 0                 2600000000
      CURR ACCT   10-Y  10-Y  CRC    24 $1500
A     SECURITY PACIFIC NATL  3110954 0                 260000000000000
      CURR ACCT   12-82 2-81  CRC   REV $2000    $0  4-09-84           CCC
A     FIRST INTERSTATE         3270827 2                 2600000000000000
      CURR ACCT   4-84  6-81  CRC   REV $2500   $65  4-25-84           CCCCCCCCCCC
A     CARTE BLANCHE            3425200 2                 2600000000
      CURR ACCT   12-83 10-Y  CRC     1  $900   $97  12-31-83          CCCCCC
A     WESTERN AIRLINES         3457870 1                 260000000000000
      PAID SATIS  7-82  10-Y  CRC   REV $1200
A     FORD CRED                3620155 1                 26000000000000000
      CURR ACCT   12-83 2-82  AUT   48$2220$17539 12-31-83
A     GREAT WESTERN S & L      3851009 2                 2600000000
      CURR ACCT   1978  1974  R/C   30$29000
  A   AFFILIATED CREDIT        3900756 0                 26000000
      PD COLL AC  9-83  4-82  UNK   UNK  -$100
  M   HAWTHORNE MAZDA          3967586
      INQUIRY     11-22-83
  A   MAY CO                   3370519
      INQUIRY     12-26-82    ISC
  A   B OF A                  3101344
      INQUIRY     4-22-82
A     FIRST INTERSTATE         3270827 2                 26000000000000
      PAID SATIS  7-82  UNKN  CRC   REV $2000
  M   CO SUP CT ANYWHERE CO  3010000 0                 0000000000001
      JUDGEMENT                                $2000 STATE TAX

------END
```