

Your Rights as a Phone Phreak

by Fred Steinbeck

"Oh, I'm not worried. They can't tap my line without a court order." Ever catch yourself saying that? If so, I'll wager you don't know too much about the laws that can prove to be the downfall of many a phone phreak. But you are wagering your freedom and money that you do know. Odds are you don't. At least, I didn't, and I had a very painful experience finding out.

Let's take a look at Federal law first. Section 605 of Title 47 of the United States Code (i.e., Federal law) forbids interception of communications, or divulgence of intercepted communications, except by persons outlined in Chapter 119, Title 18 (a portion of the Omnibus Crime Control and Safe Streets act of 1968). Section 2511 (2)(a)(1) of this section says:

"It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of any communication common carrier, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the carrier of such communication..."

The authorization stated in that subsection permits agents of communication common carriers (i.e., Telcos) not only to intercept wire communications where necessary "to the protection of the rights or property of the carrier", but it also authorizes such an agent to "disclose or use that communication." Fun, huh? That's not all.

In the case United States v. Sogden, a case which was upheld by the Supreme Court, the following ruling was made:

"For an unreasonable search and seizure to result from the interception of defendant's communication, he must have exhibited a reasonable expectation of privacy. Where, as here, one uses a communication facility illegally, no such expectation is exhibited."

This means that when you make a free call, you have waived your right to privacy. In other words, without pay, your rights evaporate.

The only limitation upon monitoring and disclosure is that it must not be excessive. For example, in Bubis v. United States, the phone company monitored all of the defendant's phone calls for a period of four months. The defendant's gambling activities were revealed by this monitoring, and this information was furnished to the U.S. Attorney's office. This resulted in the defendant being prosecuted by the District Attorney for violation of the federal laws against using interstate telephone facilities for gambling. The court acknowledged the right of the phone company to protect its assets and properties against the illegal acts of a trespasser, but ordered the evidence suppressed because (1) the extent of the monitoring was unnecessary, and (2) the defendant's prosecution for violation of the gambling laws had "no relationship to protecting the telephone company's property."

This was before the Omnibus act. As it happens, though, the Omnibus act was intended to reflect existing law, and therefore, changed nothing (pretty good, huh?). In United States v. Shah the court said (referring to the situation of inadmissible evidence in United States v. Bubis), "Thus it would appear that if the tape recordings of the defendant's conversations had been limited by the phone company to establish that the calls were in violation of the subscription agreement (i.e., were illegal) and to the identification of the person using the phone, and for those purposes only, then the tapes would have been admissible against the defendant." The court went on to say that this was

In talking with them, be civil (i.e., say Hello, talk about the weather, etc.) but say nothing pertinent to your case. They will often tell a large part of their evidence without any prodding, and at the end, will ask you some questions. You are not obligated to answer any of these questions.

At the very first signs of trouble, stop making free calls, and move anything illegal you have to a friend's house. They may not get a search warrant, but better safe than sorry.

TPC can make life miserable for you, and they don't often prosecute unless they're sure of winning, which is pretty much always. Therefore, you must make it either not worth their while to prosecute, or worth their while not to prosecute. The best bet is to try to get them to settle before going to court by offering reimbursement and being nice to them. If you appear genuinely sorry, they may not prosecute.

Failing that, be a low-down bastard and make as much trouble for them in court as possible. Just remember: technology is on your side, and that's better than God.



HACKING DUN & BRADSTREET

by BIOC Agent 003 & Tuc TucBBS

Dun & Bradstreet is like TRW, except it is for businesses. It allows users to check out financial records as well as other statistics about a company. It is everything you always wanted to know about your local rip-off store (owner) or a corporate piglomerat, but were afraid to ask.

To logon dial one of their local #'s such as: (212) 619-4600 or (201) 277-4000, use Telnet (C 20188), or Tymnet (TERM: A, LOGON: RPTS, PASS: NOW)

Once on type RPTS <CR>, followed by another <CR>, followed by PRNT <CR>. It will then ask you for your password which is in the format of: #####/PASSWORD

For example, 001779 is a demo account, the old password was DEMO but they got smart. If this still worked you would type 001779/DEMO. See if you can figure out a new password for this account.

Once you have a password, it will give you a short menu such as: "P=PAR REPORT, D=DFT ORDER", etc. When it says ENTER SELECTION:, type P. It will then say ENTER INQUIRY:, here you type the business name or characters to search for. It will then say ENTER CITY:, and enter it. Enter the 2-letter state abbreviation when it says ENTER STATE:. At the next question, answer P for par. Then enter a <CR> when it asks for an endorsement. It will then give you a list of businesses that match the letter(s) that you inputted. Type the # of the one that you want. When it says ENTER SELECTION: again, type F for a Full report. When it says PRINT NOW?, type Yes and whalla, a perfect 50-column printout on the business. This is just the basic report; fool around with the menus for other options.

GATHERING WITH FRIENDS - EDDIE'S ON A FRIDAY NIGHT

I got some flack from my article a few issues back called "How To Infiltrate TAP", wherein I mentioned how to find our Friday night watering hole in Greenwich Village. Most of it was from the Friday Night Irregulars, the guys that "usually" show up for a brew and some onion rings. In fact, there's been a little less elbow room around the table on Fridays, but folks like Tuc, and BIOC Agent 003 have submitted some good articles, so hopefully we can get those who come down to write for us. That's why I'm mentioning it again.

This doesn't mean that if you can't make it to Eddie's at 14 Waverly Place that you can't write for TAP. Anyone who can set their typewriter margins to 50 characters wide will probably wind up with stuff published in TAP. These days we can use some short filler items too, so please submit anything!

Eddie's is on Waverly Place between Broadway and Washington Square Park, both large landmarks that even Brooklynites can direct you to. If I say any more than that the RR train gets you the closest, the Friday Night Irregulars will probably have my scalp, since it's getting crowded enough on Friday's already. I try to make it most weeks myself, but holiday weekends usually find me visiting friends out of town.

Those people that come by TAP's mailing address are, for some reason, surprised when Room 603 turns out to be simply a telephone answering and mail service (or more formally known as a "mail drop"). Another method of reaching me, however, is MCI Mail, where a "TO" address of "CHESHIRE" will get a mail message to me.



The Hobbyist's Newsletter for the Communications Revolution

Jan-Feb 1984 Issue 98

Indeed the case in United States v. Shah, as the phone company only monitored for 7 days, and the tapes were of 1 minute duration at the beginning of any illegal call.

So what can they do? Well, several things. First, they can put a dialed number recorder (DNR) on your line if they suspect toll fraud. There are several varieties of DNR's floating about. The most common can do the following: print Touch-tone digits sent, print MF digits sent, record presence of 2600 Hz on line, and activate a tape recorder for a specific amount of time (generally 1 to 2 minutes) when some specific event occurs, such as 2600 Hz being blasted into the line.

DNR's seem to be fairly standard procedure. That is, almost all the Telcos use them when they suspect fraud. As long as they do not record the entire conversation, or conversations that are legal, there is nothing illegal about DNR's. DNR's are also used to detect fraud using specialized common carriers (e.g., Sprint, MCI, etc.), by watching you dial the local dialup number, followed by your (illegal) access code and destination number. They do not need a court order to place a DNR on your line.

If they can record voice on your line, they can record data just as easily. So if you call bulletin board systems and have a DNR on your line, be aware that any logins you have made have probably been watched by the phone company, and they probably know any passwords you have used.

The purpose behind all this DNR bullshit is to establish your identity. I suppose a possible defense against this is simply not to talk for three minutes after the connection is established. Might be kind of hard to do in practice, however.

Contrary to popular believe, TPC does not make "midnight visits" to your house to arrest you. Why should they? A judicious application of their motto, "Reach out and put the touch on someone", means that they simply call from their office. If they call, try to draw them out as much as possible in a phone conversation. That is, they will keep muttering about how they "have evidence". Find out what kind of evidence. Do not expect them to be forthcoming with everything. They will almost certainly have more than what they tell you.

Their standard position is to prosecute all offenders, although this varies depending on the severity of the situation, as well as the age of the offender. They tend to always prosecute adults, while they are receptive to pre-trial offers made by juveniles. They may want to talk with you in person, ostensibly to give you a chance to explain why the 300 calls to the local Sprint node came from your line. Accept this offer. Often they are more generous with their evidence in person than they are over the telephone.

If you do meet with them in person, bring a lawyer. Lawyers are expensive, but they are well worth the price. They know the law, while you don't. The investigators TPC employs are seasoned people, and usually make few mistakes, legal or technical. However, a good lawyer can spot any legal fuckups they might have made, and you should be able to find any technical ones. continued next page

HACKING WESTERN UNION'S EASYLINK

By BIOC Agent 003 & Tuc TucBBS

Easylink is a system that allows you to send Telex, Telex II (TWX), mailgrams, telegrams, cablegrams, and a few others.

First, either dial the local # or (800) 325-4112 (for 300 baud). It will respond with EASYLINK, followed by ID? At this point, you should enter the code, which is in the format of:

01 ESL##### USERNAME.PASSWORD

Where: 01 - says your are using full duplex ESL - says your are using Easylink ##### - a 6 digit account code USERNAME.PASSWORD - just that

Once on, it will respond with a connection #, the date, and time. You will then see PTS, which stands for Proceed To Select. You can then type "/HELP" to see what you can do with the system. If you want to send a Telex, type the telex # followed by a plus(+). It will then respond with GA which stands for Go Ahead.

Now type in the text. To send the text and stay on Easylink type LLLL; to send it and log off type MMMM. To abort the message, type EEEE. It will then say either "ACCEPTED" followed by a # or "MESSAGE DISCARDED."

If you want to send a mailgram, type:

/ZIP WHO TO ADDRESS 1 ADDRESS 2 (optional) CITY ST ZIP+

Make sure that the zip is followed by a plus (+). At the GA, type in the message and terminate it with LLLL. With mailgrams the return address belongs to whoever owns the account. More on changing this info in part II, or if you penetrate the system before then, write to us c/o TAP.

For info on sending telegrams, editing, etc., type "/HELP" after any PTS prompt and it will give you a rundown.

If you just want to check out the system and practice, log in using: 01 USR999999 TEST.TEST This is their demo password. It no longer allows you to send actual letters, though.

Another WU system that uses the same password format is FYI (For Your Information). It is at (800) 325-NEWS (6397) and it carries UPI news and other "goodies." Once on type CATALOG or UPIINDEX for help. Unfortunately, the demo password no longer works on this system.

4,700 AT&T Credit Cards Mailed to Wrong People

REDMONSTER, N.J. (AP)—American Telephone & Telegraph Co. officials said Wednesday that they have mailed an estimated 4,700 telephone credit cards to the wrong customers, and appealed to consumers to "be honest" and not use them fraudulently.

AT&T was in the process of mailing out 47 million credit cards when customers began calling to say that they had received cards with the wrong name and telephone number, said Maxwren Dvornik, spokeswoman at AT&T's Communications division headquarters here.

AT&T spokesman Jerry Santos said the firm believes the problem is limited, and that it will not be necessary to stop the mailing of those not yet sent. He said the company estimated about 0.01%—or 4,700—of the cards had been incorrectly mailed. He said he did not know how that figure was determined.

Dvornik said the firm has set up a hot line for customers to report receiving wrong cards, but that it was too early to tell how many of those calls had come in.

Dvornik said using the toll-free service—1-800-CALL-ATT—to report the credit card problems will not increase company costs because it had set up that system nationwide before the first cards were mailed in order to answer questions about the AT&T breakings.

An operator who answered the toll-free number Wednesday said customers who report receiving the wrong card are told to destroy the card immediately and that they will be issued a new card.

Dvornik said the company will not have a firm grip on the problem until the first round of bills comes due March 1 under the new system put into effect when AT&T was broken up Jan. 1.

The problem arose when some cards were placed in the wrong envelopes for mailing and when some customers moved and cards were sent to their old addresses, she said.

The Coming "Snowstorm" in Telecommunications

by Cheshire Catalyst

This is the first issue of TAP since the breakup, and I felt an article on the "phreaks eye view" of the divestiture would be in order.

In 1897, there were 7 local telephone companies in New York City. The snowstorm of that year caused great damage to the aerial wires, bringing them all down. The president of the largest of the 7 called in the presidents of the other 6 and suggested that they pool their resources, and become one Telephone Company. This was how the New York Telephone Company (now owned by Nynex) came to be.

We all know the shitty quality of Sprint, MCI, and the others, as well as the chaos of the split of the Bell System. As a phone phreak, I'm expected to hate The Phone Company. After all TPC has for decades been "The company you love to hate." But the Network, ah, the network!

I doubt if statistics have been kept as to how many phone phreaks were caught because they reported problems to internal repair numbers they shouldn't have known about. In fact, as a "civilian", they shouldn't have even realized what the problem was! But phreaks love The Network (I'm talking REAL phone phreaks here, not just Sprint & MCI crackers). Now that The Network is being broken up into the networks, the phreaks are worried about the real harm that will come to phone service in this country.

Regulatory bodies are realizing that many divestiture decisions are ludicrous in light of the amount of expertise being by The Public to keep track of all that is happening. Here in New York City communities, Congresspeople are using their legislative bulletins to inform citizens of the meaning of divestiture. They realize that this "consumer awareness" type of information is not in the financial interest of the consuming public, and that the Public Service Commission doesn't have the resources to get this information out. While The Public has hated The Phone Company for years, it was at least "the devil they knew". Now there is so much they are expected to know, that they are finding out they can't handle it.

For example, if there is a problem with your line, the local Telco says it will fix it for free, but if the problem turns out to be your premise station equipment, then they will charge you for the service call. Likewise, ATT Information Systems (owners of the telco's former leased equipment, and present lessors) will fix your phone for free, but if the problem turns out to be the line, and they've wasted a service call, you will also be billed. What little old lady in Murray Hill living with her two cats will be able to figure out whether it's the phone or the line, and stand to be socked with a \$40 charge if she's wrong. Little old ladies make up a big constituency, and I think that Congress will step in 5 to 10 years down the line when the "snowstorm" of mail gets to be too much to ignore. I'd almost dare say to look for it to be an election issue in the 1988 presidential election.

I don't pretend to know the answers, but the public will demand it's telephone service be brought into line in a few years. Heaven help the Congress when that mob gets ugly.



MCI