
# *Exploding The Phone*

www.explodingthephone.com

Bibliographic Cover Sheet

**db228**

Title **Beating the blue-box bandits**

Publication *IEEE Spectrum*

Date 1972-08-00

Author(s) Eleccion, Marce

V/I/P p. 52

Abstract Overview of phone phreaking and countermeasures written for an engineering audience. Discusses verification, loop arounds, blue boxes, etc. Mentions a blue box built in a Navy shipyard. Mentions Captain Crunch, Midnight Skulker and others. Includes photos of various phone phreak technical documents. Interviews several telephone company and Bell Labs engineers. Provides statistics on fraud.

Keywords Tom Powers; Kenneth D. Hopper; Joseph F. Doherty; Harold E. Brown; blue box; black box; mute box; cheesebox; cheese box; Navy shipyard; Captain Crunch; Dr. No; The Snark; Midnight Skulker

Source ProQuest

# Beating the blue-box bandits

## The answer to any system defrauding seems clear—vigorous prosecution and greater engineering and moral responsibility

Marce Eleccion Staff Writer

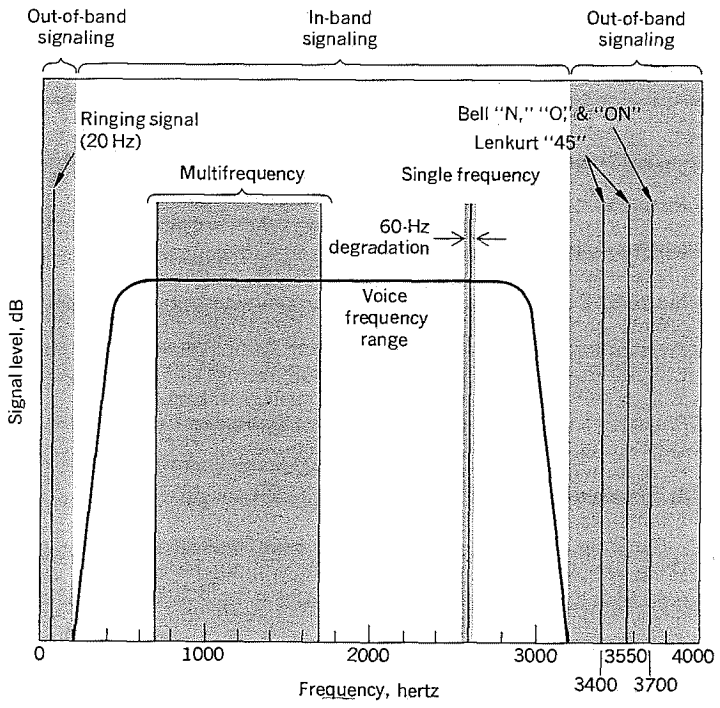
As if the telephone utilities didn't have enough to worry about, it seems that a new breed of defrauder has emerged over the past decade to criminally intrude upon a particularly vital part of the telephone system—the toll network. Armed with hardware that ranges from the shoddiest of devices to the newest in integrated circuitry, these "phone phreaks" are able to call virtually around the world via the telephone network—without paying. The methods that are currently being used exploit an unfortunate vulnerability that exists in the present toll dialing telephone system: the inclusion of control signaling within the voice-frequency band.*

What is basically causing concern among the telephone utilities is the fact that the single-frequency (SF) and multifrequency (MF) toll-traffic signaling tones, which are presently being carried within the voice transmission band (see Fig. 1), can be generated directly from the more than 100 million telephone instruments within the easy grasp of practically the entire U.S. populace. Although the economic and technological considerations that led to the eventual decision to install such a system (see box on dialing and the telephone network) a few decades ago may have been justified at the time, the telephone companies are now beginning to regret ever having opted for such an obviously fallible method of toll signaling.

The problem, of course, arises when individuals out to beat the phone system attempt to initiate SF and MF signaling on their own, thus preempting the role of the toll operator who normally directs these network control signals. The device that these defrauders (who, like most criminal elements, represent only a small percentage of the population) use is called a "blue box," supposedly because the first such unit discovered was that color (and also to differentiate it from black boxes, cheese boxes, etc.). Essentially a tone generator, the blue box has been found in all forms, shapes, and disguises (some even designed to self-destruct). The only unit that this writer has seen (at AT&T) was clandestinely constructed in a Navy shipyard and represented magnificent craftsmanship on the part of the builder—a somewhat dubious tribute to the ingenuity of some of these phone defrauders.

Actually, this type of phone phreak—the MFer or blue-boxer—belongs to a larger category of telephone defrauders (see box, page 53), all practitioners in the art of "ripping off" the phone companies. In the recent literature publicizing these "phone phrauds" (a more accurate epithet), the implication is that they are a loosely organized but glamorous camaraderie. Nothing could be

**[1] In-band and out-of-band signaling frequencies in the telephone network.**




* Ironically enough, the basic concepts of this transmission method were divulged by the largest of the telephone utilities, AT&T, in a paper that appeared some years ago in the *Bell System Technical Journal.*


**The cause of growing concern on the part of the telephone companies, the phone phreak's "five-foot bookshelf" is beginning to fill in from the most unexpected sources.**

further from the truth! Rather than the antiestablishment avant-garde these defrauders pretend to be, they are in essence violators of the public faith, since their crime is directed at the telephone community as a whole—the user as well as the carrier.

Certainly, such sobriquets as Captain Crunch, Dr. No, The Snark, and Midnight Skulker contribute a colorful image to these supposed modern-day Robin Hoods. When one considers the fate that befalls them, however, the color begins to fade. Captain Crunch (derived from the whistle found in the breakfast cereal of the same name that generated 2600 Hz, a traffic-signaling tone), one of the original phone phrauds, was recently arrested by the FBI and faces prosecution under Federal statutes. Individuals said to have built fraud devices for elements of organized crime have either disappeared or died violently—a serious deterrent to those contemplating making such devices for others.

### The extent of phone defrauding

Although the increase of overall phone fraud since 1965 has been estimated as high as 700 percent, there are indications that the phone companies are beginning to win the battle against offenders, mainly because of an aggressive toll-fraud program they were wise enough to institute early in 1971 and the development of highly

### Boxes galore

"Blue box," "cheese box," "black box," and "mute box" describe some of the devices that phone phrauds have used to cheat the telephone companies. They go beyond the cruder defrauding tactics of "box stuffing" and outright coin-box tampering. The cheese box, one of the earliest devices, was often used by bookmakers to conceal their illegitimate operation. It worked by connecting two phones in such a manner as to redirect all incoming calls to a second remote phone; when the authorities located the first phone, they found they were disconnected from the real culprit. The black box (also known as the mute box, among other names) enables the user to receive free incoming calls. This method, involving circuit modifications to defeat toll billing, was the subject of a recent article in **Ramparts**; the issue was recalled since it was in obvious violation of the California Penal Code (see tinted box, p. 57).

By any name, the boxes just described can be called by a single adjective—illegal, and the penalties for their use by another—severe!

## Multifrequency dialing and the telephone network

The growth of the telephone communication system is one of the great modern success stories. The simple procedure of dialing a 7–13-digit number and talking across continents has become so commonplace that one forgets the complexity of the system itself.

An idea of the basic elements involved in the switching network comprising the direct distance dialing (DDD) system of North America can be seen in Fig. A. Basic to this system are the up to $10^4$ subscribers who may be located within one central (end or exchange) office of a local area. It is through these central offices that a user is automatically switched to the high-usage intertoll routes that complete a toll call; such trunks use toll cables, coaxial cables, and point-to-point microwave transmission. Overseas connections can be made through submarine cables, satellites, and radio transmission.

The rapid growth of telephone usage in the United States alone can be seen from a comparison of the statistics over the decade from 1959 to 1968. During that period, telephones in use increased 55 percent (from 66.6 million to 103.8 million). By comparison, the world increase for this period was 78 percent (from 124.8 million to 222.4 million). In 1968, there were a total of 22 000 central offices in the United States. Given a theoretical $10^4$ subscribers for each exchange, the theoretical capacity in that year was over 200 million instruments.

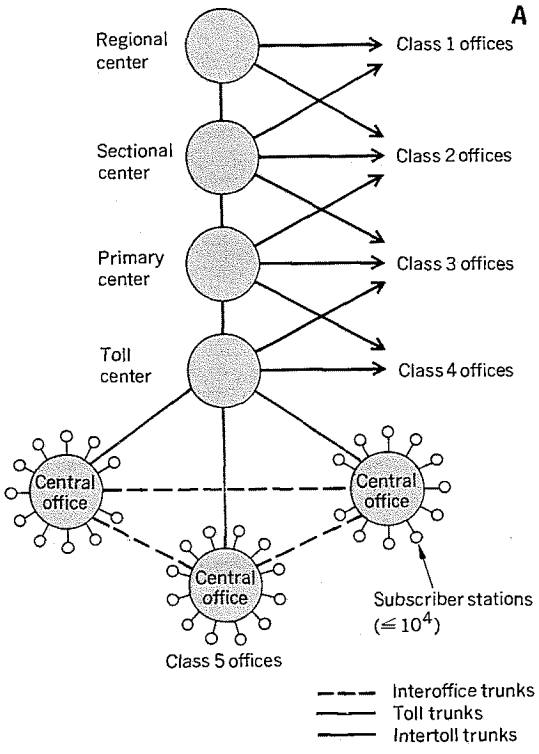
Technical improvements have been made in the telephone instrument itself. Originating with the early magneto/local-battery system in which the call was completed by a switchboard operator, this device underwent a radical change with the introduction of the rotary dial in 1895. With this dialing system, it became possible to dial a number directly by generating a pulsed dc digit. The most recent innovation—and the one that eventually led to the present phone-phreaking problem—is key-pulse or pushbutton dialing, which had been used for toll and dial service assistance (DSA) switchboards for a number of years but was withheld from consumer use because of voice-interference problems that existed.

Operating with multifrequency tone keying using ac pulses (opening the way to newer services such as computers), the pushbutton system (Fig. B) utilizes eight frequencies within the voice band (different from the six toll-traffic signals) over a 16 button format (only 12 are actually used for AT&T's Touch Tone® telephone sets). Initiation of such fast (any digit can be transmitted in the same time it takes for transmitting "1" on a rotary dial) and accurate number generation was deemed a necessity because of the increased telephone traffic and the higher speeds of future electronic switching systems.

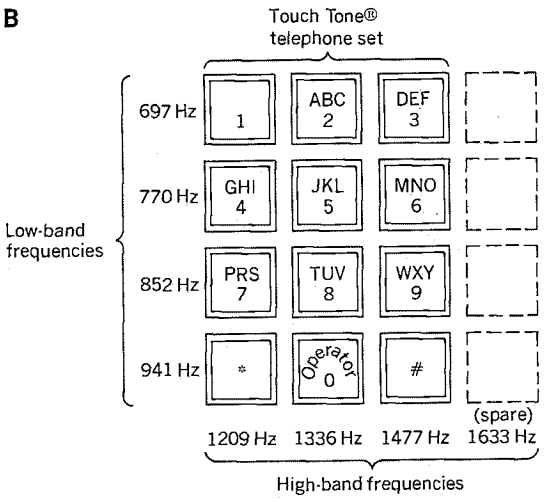
At the present time, electronic switching systems (ESS) serve only a small percentage of the U.S. telephone network, with direct-control and common-control electromechanical switching systems serving most of it. It is projected, however, that every central exchange in the U.S. will have electronic equipment by the year 2000.

Since the blue-box problem has come about as a result of the inclusion of multifrequency toll signals within the voice transmission band, the question naturally arises: "Why not separate the two?" The answer is that such a solution is already being worked on, but will require both time and large expenditures of money to implement in a system as large as the telephone network. Meanwhile, the problem must be approached in the ways described within this article.

**Elements of a telephone network.**




**Pushbutton dialing frequencies.**



effective and sophisticated detection techniques.

In the area of fraudulent credit-card and third-number calls (billings to a third number at the calling party's request), the Bell System has succeeded in halting a spiraling trend in revenue losses, as can be seen in the following:

| Year | Credit-Card and Third-Number Fraud |
|---|---|
| 1968 | $ 3.5 million |
| 1969 | 6.9 million |
| 1970 | 28.3 million |
| 1971 | 22.2 million |

Not only were revenue losses appreciably reduced in 1971 but there was a marked increase in prosecution—330 arrests and 255 convictions (with many cases still pending in the courts)—as compared with 215 arrests and 207 convictions in 1970.

Another area where losses have been substantially reduced is coin telephone larceny. In 1967, Bell System losses from this type of crime reached an all-time peak of $3.5 million, which includes equipment damage and destruction. By 1971, these types of losses were reduced to about $2 million, which was largely due to widespread use of armored coin telephones with sophisticated locks, metal-clad cables, heavy-duty dials and handsets, and single-slot coin telephones that detect and resist "stuffing" as well as slugs.

Unfortunately, the losses that are sustained due to blue-box toll frauds are difficult to estimate. Bell representatives have been quoted at a conservative figure of between $50 000 and $100 000 a year, but independent telephone company representatives give estimates as high as $150 million. The arrest and conviction record is a little more encouraging; although there were only six arrests and two convictions in 1970, there were 45 arrests and 35 convictions (cases still pending) in 1971.

Although the extent of blue-box activities has been thought to be somewhat restricted, the recent experience of a few Bell Laboratories investigators may prove to be a more accurate indicator of the numbers that are actually involved. In visiting a large eastern engineering school to query three students who were active MFers, the Bell group was informed that approximately 100 blue-box devices were in use at this one school alone!

If one can believe the literature, the ramifications of blue-boxing exceed the ability to just make free calls. According to at least one source, phone phrauds are also able to intrude upon the privacy of time-shared computer banks that are accessed through the common carriers. In querying the director of engineering of a major software corporation, this writer was informed that it is indeed possible to do so, especially if one learns the control format of a particular system as a former or present user of the computing service. However, even if an intruder is able to breach the top two levels of security, there are additional levels within the file system itself that are known only to the user himself, making it an exceedingly difficult feat to achieve actual intrusion. As if that weren't enough, truly critical data can be stored in a scrambled format, with the chances of deciphering the algorithm scheme virtually nonexistent.

Given the undaunted spirit of a resourceful intruder, however, it is feasible that he will continue his attempts at cracking the code. If this happens, the abnormal access condition is easily detected by error-signal analysis and corrective measures may be taken by the computer firm. In addition, any line access to a computer port must be accompanied by suitable signaling conditions or it will be shut off; hence a phone phraud must also be in possession of expensive data equipment. Of course, the use of leased lines and fully dedicated file areas preempts any nonphysical access to a computer bank.

Another blue-box intrusion that has been reported is that of wire tapping. The truth of this claim seems in doubt, however, although it is possible for a verification operator using a verification trunk to intrude upon a subscriber's phone conversation in an emergency, a situation many readers may have experienced.

Other blue-box variations that have been speculated upon include the more expensive telephone-answering devices that can be queried for messages remotely by the user after signaling with a tone blast. Without direct information, however, the chances of selecting a single or multifrequency tone from the telephone transmission bandwidth of 200–3200 Hz are pretty slim.

### Detection, apprehension, and prosecution

Not surprisingly, the detection methods that are being employed by the telephone companies are not being divulged to the general public (this writer included). An area of obvious great importance, the detection of any criminal activity is dependent on many factors: defrauder error, suspicion based on calculated hunches or calling patterns, billing analysis, or even informants.

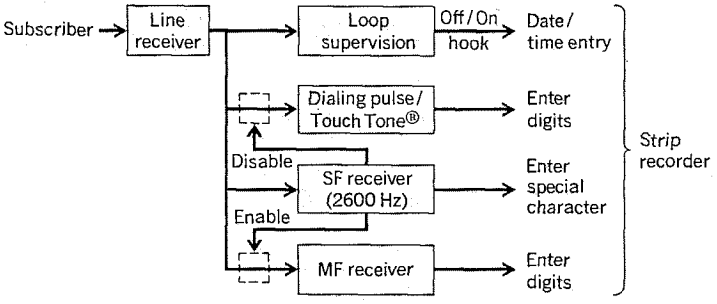
Specific and extremely specialized equipment may also be used, such as that needed for SF/MF detection on a telephone line. What this device does is detect the presence of an unusually long burst of 2600 Hz on a line and trip a counter that records the length of the call, as well as other data. A system that employs this method could operate as described in Fig. 2.* Here, a supervisory circuit detects the off- and on-hook conditions of the telephone and stamps a date and time entry on a recording strip. The equipment then records the legitimate toll number that is dialed (usually a charge-free number), the SF and MF signals illegally entered onto the line, and the conclusion of the call.

According to Bell Labs experts, the SF/MF method of evidence gathering is only one of a great number of detection tools that are at the disposal of security and law-enforcement agencies, with many techniques displaying a high degree of sophistication.

The countermeasures problem confronting today's

* Northeast Electronics Corporation, Concord, N.H.

**[2] Simplified system for SF/MF signal processing.**



### Powers on fraud

There's no doubt that there's a problem with fraud in most large systems in the country today, whether they're telephone networks or computer networks or whatever. We've been concerned about fraud in the Bell system from many points of view for many years, originating with the very coarse, gross kinds of fraud, if you like, of people billing calls to telephone numbers that aren't theirs (say to your home phone number or to your credit-card account number) or the strong-arm kind of business where someone takes a coin telephone box and breaks it open. I'm not making too much of a distinction between vandalism per se and fraud per se. I'm thinking only about ways in which people manipulate the system in order to escape the legal obligations to pay for the services that they're provided.

Since basic telephone services are paid for by the great mass of consumers through tariffs approved by the State utility commissions and by the Federal Communications Commission, someone pays for every call. If the person who makes that call doesn't pay for it, then the net result is a slight increase in the average cost of calls made by all the honest customers.

The primary question is: Do the people who get the service pay for the service?

We talk blithely and with sincerity about the older people on pensions who pay telephone bills every month just as we do. And there are a lot of people like that, including, perhaps, our parents, and anything that makes the cost of local service go up tends to work to their disadvantage. That's one of our concerns.

We do view fraud as a problem. People have grown more sophisticated, more information on our system has been published (and we ourselves published a great deal of it in the past), college students and others have been able to take advantage of electronics, which many *Spectrum* readers, including me, have helped to bring into being. Things like integrated circuits and transistors now exist, leading to a much higher level of sophistication in circuitry than was extant in the country perhaps two decades ago. Certainly then, people have become much more clever at working the system in fraudulent manners.

And so the problem is growing. But at this time, it's not a problem that's about to sink the telephone utilities, by any means. We have many projects here at the Bell Labs and there are many in the Bell System that are occupying a lot more of our time and money and effort.

It certainly is not insignificant either. It's not at all trivial; we are concerned about it. AT&T of course is carrying the burden from the point of view of legal remedies to the problem—the apprehension and prosecution of people who are involved in defrauding the telephone companies—and in providing the systems consideration and direction to our development efforts.

*Tom Powers*
*Director, Telephone Laboratory*
*Bell Telephone Labs, Holmdel, N.J.*

telephone utility are enormous, especially with the increased availability of modern electronics gadgetry (see "Powers on Fraud," above). Tom Powers of Bell Labs has summed it up in this way:

"Whenever information as to how a system is intended to work comes out in any fashion, a few people very quickly find a way around it. It seems that, no matter how smart we are, it doesn't take long until someone figures out a way to break the code and the losses start going up again. . . . We're very much concerned about tipping our hand and giving away the combination to the safe."

The temptation to defeat the phone system at this counter-countermeasure game may seem irresistible to some; if so, they would be wise to consider both the penalties that must be exacted and the undaunted resolution of the phone companies. Joe F. Doherty, director of corporate security for AT&T, has stated his position in prosecuting phone defrauders most unequivocally:

"We are prosecuting aggressively and without any exception. We have a Federal felony statute, we would like felony laws in every state, in addition to existing laws that make fraud a violation that is other than just a misdemeaner. . . . We're getting more interest out of the FBI and we're getting more felony prosecutions. So when these people are convicted of a Federal felony, they've got the stigma for the rest of their life."

What Mr. Doherty was referring to was Title 18 of the United States Code, specifically paragraph 1343 entitled "Fraud by Wire, Radio, or Television." (See box, p. 57.) The wording of the pertinent sections of this statute may seem like legalese to some, but the meaning of the penalties for those prosecuted for this type of fraud come through loud and clear—a fine of "not more than $1000," imprisonment for "not more than five years," or both! (Earlier Federal statutes that attempted to control fraud in the communications field included Section 605 of the 1934 Federal Communications Act (Title 47, U.S.C.), which was entitled "Unauthorized Publication or Use of Communications.")

The tinted box on page 57 contains several excerpts from the Federal criminal code and various state penal codes dealing with wire fraud. It should be emphasized that, even though only about half of the states specifically proscribe the possession and/or use of phone fraud devices, the Federal statutes, which are much stronger than most existing state laws, provide an effective and forceful means of dealing with this type of fraud. Such federal jurisdiction brings with it an exemption to extradition procedures, reduced evidential problems, and of course the threat of surveillance and eventual apprehension by the FBI.

Concerning the actual printing of written material advocating (as some of the more nonconformist magazines and underground newspapers have been doing with increasing frequency) the defrauding of telephone companies, the statutes that have been passed in California, Georgia, Kansas, Maryland, and Virginia (Gov.

## Title 18, United States Code (1958 Edition)

**§1343. Fraud by Wire, Radio, or Television**

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined not more than $1000 or imprisoned not more than five years, or both.

## California Penal Code (1965 Cum. Supp.)

**§502.7. Obtaining Telephone or Telegraph Services by Fraud**

(a) A person who, knowingly, willfully and with intent to defraud a person providing telephone or telegraph service, avoids or attempts to avoid, or aids, abets or causes another to avoid the lawful charge, in whole or in part, for telephone or telegraph service by any of the following means is guilty of a misdemeanor:

(1) By charging such service to an existing telephone number or credit card number without the authority of the subscriber...; or

(2) By charging such service to a nonexistent telephone number or credit card number, ...; or

(3) By use of a code, prearranged scheme, or other similar stratagem or device whereby said person, in effect, sends or receives information; or

(4) By rearranging, tampering with, or making connection with telephone or telegraph facilities or equipment, whether physically, electrically, acoustically, inductively, or otherwise, ...; or

(5) By using any other deception, false pretense, trick, scheme, device or means.

(b) A person who (1) makes, possesses, sells, gives or otherwise transfers to another, or offers or advertises an instrument, apparatus or device with intent to use it with knowledge or reason to believe it is intended to be used to avoid any lawful telephone or telegraph toll charge...; or (2) sells, gives or otherwise transfers to another or offers or advertises plans or instructions for making or assembling an instrument, apparatus or device described in paragraph (1) of this subdivision with knowledge or reason to believe that they may be used to make or assemble such instrument, apparatus or device, is guilty of a misdemeanor. ...

(e) If the total value of all telephone or telegraph services in violation of this section aggregates over $200 within any period of 12 consecutive months during the three years immediately prior to the time the indictment is found..., a person guilty of such offense is punishable by imprisonment in the state prison not exceeding five years, or by imprisonment in the county jail not exceeding one year, or by fine not exceeding $5000, or by both such fine and imprisonment.

**§640. Wire Tapping; Use of Information; Conspiracy; Punishment**

A person who, by means of any machine, instrument, or contrivance, or in any other manner, willfully and fraudulently, or clandestinely taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument under the control of any telegraph or telephone company; ... or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any telegraph or telephone wire, line, or cable, ... is punishable by imprisonment in the state prison not exceeding five years, or imprisonment in the county jail not exceeding one year, or by fine not exceeding $5000, or by both such fine and imprisonment.

## Arkansas Statutes (1947 Annotated): Title 41—Criminal Offenses

**§41-1956. Telecommunications—Obtaining Service with Intent to Defraud—Prohibited Acts**

Any individual, corporation, or other person, who, with intent to defraud or to aid and abet another to defraud any individual, corporation, or other person, of the lawful charge, in whole or in part, for any telecommunications service, ... by any of the following means may be penalized as provided in §41-1959 of this act:

(a) By charging such service to an existing telephone number or credit card number without the authority of the subscriber..., or

(b) By charging such service to a nonexistent, false, fictitious, or counterfeit telephone number or credit card number, or to a suspended, terminated, expired, cancelled, or revoked telephone number or credit card number, or

(c) By use of a code, prearranged scheme, or other similar stratagem or device whereby said person, in effect, sends or receives information, or

(d) By installing, rearranging, or tampering with any facilities or equipment, whether physically, inductively, acoustically, electronically, or

(e) By any other trick, stratagem, impersonation, false pretense, false representation, false statement, contrivance, device, or means.

**§41-1959. Penalty for Fraudulently Obtaining Telecommunications Service**

Any person violating the provisions of §41-1956 of this Act shall be guilty of a misdemeanor and upon conviction shall be subject to a fine of not more than $100 or imprisonment for not more than 30 days if the amount of the telecommunications service obtained by such use does not exceed $35, or by a fine of not less than $100 nor more than $500 or imprisonment of not more than one year if the aggregate amount of the telecommunications service obtained by such use exceeds $35, or by both such fine and imprisonment.

Rockefeller recently vetoed a similar law in New York) prohibiting this are expected to be court tested within the next few months. Organizations that advocate similar disruption of the telephone system will probably fall under this jurisdiction.

### Other problems

Those who examine the literature will find many claims ascribed to the phone phraud and his blue box, some quite unbelievable. Having no means of verifying the truth or untruth of these dramatic feats, this writer questioned several persons at Bell Labs involved in finding solutions to the problem: Tom L. Powers, Director, Telephone Laboratory, BTL, Holmdel; Harold E. Brown, Head, Station Studies Department, BTL, Holmdel; and Kenneth D. Hopper, MTS, BTL, Holmdel. Questions and answers follow.

*Question:* The problem of phone fraud seems to have serious ramifications in the field of carrier-serviced time-shared computing. Is it really possible to write out a clever-enough program that will decipher the code words needed to gain access to time-shared computer banks?

*Answer:* We have no technical data that would let us have a valid comment on that fact. Of course, the scuttlebutt is that the answer is yes, that people who work very long and hard at this can find ways to get around the security of some computer systems, and a large number of people are concerned about this problem, including the government, since they probably have more data than anyone else stored in computer data banks.

*Question:* How much truth is there to the statement that four phone phreaks with sufficiently sophisticated equipment can tie up the entire United States wire communications network?

*Answer:* I think it's highly unlikely, although it's sort of risky to say that, with 200 million people in the country, there isn't anyone anywhere smart enough to ever do it. . . . It would be extremely difficult. Right now, I think it's probably fair to say, we don't know of any very easy way to do it.

*Question:* What about these closed loop-arounds that enable phone phreaks to establish unlimited party-line conferences?

*Answer:* Well, that's an area that it turns out there are things that can be done and are being done to make that much less of a problem to us. Of course, in getting rid of loop-back-type systems, it causes us a little bit of a problem, since we've got to go to somewhat more clumsy methods that are more costly. But I think the problem is going to dwindle away very quickly.

*Question:* It's been claimed that phone phreaks have the capability of tapping into private telephone conversations; is this true?

*Answer:* I think they're alluding to verification access. At this time, we know of no verification trunk that is accessible by either a subscriber-dialable code or by an operator-dialable code in any part of the Bell System. [In] every verification circuit that is accessed through an operator's position in this manner, the interface is kept well controlled.

*Question:* What about the deception of operators and switchmen to gain entry to unauthorized trunks?

*Answer:* There have been measures to tighten up such arrangements.

Perhaps the answer to the entire question of telephone security—and for that matter any system security—lies in the candid observations made by Mr. Powers as our meeting came to a close:

"Anything that makes the [fraudulent] user different from the average user provides a handle that we can go to work on. . . . We've found ways of using many of the things that are in the toll network for other purposes to give us a handle on fraudulent calls, and I'm sure that other ways will come up as we turn our attention more and more to this area. . . .

"It's just the growing feeling that it's kind of fun to outwit the system, and I guess it is. It's not just our system, however, it's every system that comes along. In a sense, the revenue losses affect not only our company's costs, but eventually the rates that our customers have to pay.

"From a philosophical point of view, the kind of change in morality that makes beating a system seem fun to some people is a real concern to us. It's going to be very difficult in the future, I think, to design systems that are so simple and convenient that even the most poorly educated . . . member of our society can use them, and yet are so foolproof that even the most highly sophisticated technology bug in the country can't find a way around them.

"And yet, that's really, I think, the challenge that we have if we're going to provide communication services and, at the same time, keep the cost low enough so people can universally afford these services."

### The solution

This examination of the telephone defrauding problem has turned up various answers—some of which may very neatly apply to the general problem of system defrauding. Aside from the specific, short-term solutions, such as the installation of tamperproof coin phones and the implementation of detection devices to monitor the illegal use of telephone traffic signaling, any long-term solution must be approached from three vantage points: those of the carrier, the user, and the Government.

From the point of view of the telephone system itself, it seems imperative for the system designer—the engineer—to examine the societal implications as well as the cost–benefit factors. Certainly, the present blue-box dilemma would not have arisen if the system designer had not included traffic signaling within the voice-frequency band, thus inviting fraud. On the other hand, there will always be the temptation to "beat the system" no matter what its degree of sophistication. So the engineer must choose the right tradeoffs between system complexity and user cost, and system vulnerability and system cost.

For the user, the "solution" to system defrauding of any type lies in greater moral responsibility. Rampant antiestablishment feeling may be partly to blame (although personal gain should not be discounted as part of the defrauder "psyche").

The Government's role in halting telephone fraud has been one of vigorous apprehension and prosecution, aided by the telephone utilities' step-up in detection activity and their strong desire to act as witnesses for the prosecution.

In the face of such a three-pronged assault, there is good reason to expect a victory in the war against the "blue-box bandits."