Exploding The Phone

www.explodingthephone.com

Bibliographic Cover Sheet

db385

Title	**The Blue Box and Ma Bell**
Publication	*Radio Electronics*
Date	1987-11-00
Author(s)	Friedman, Herb
V/I/P	p. 49
Abstract	Historical, technical overview of blue and red box theory of operation. Includes schematics/block diagrams.
Keywords	Automated message accounting (AMA); blue box; red box
Notes	The author makes a number of unsubstantiated claims and also confuses red boxes with black boxes.
Source	Alan Rubinstein

48783

Radio Electronics

SURFACE-MOUNT TECHNOLOGY

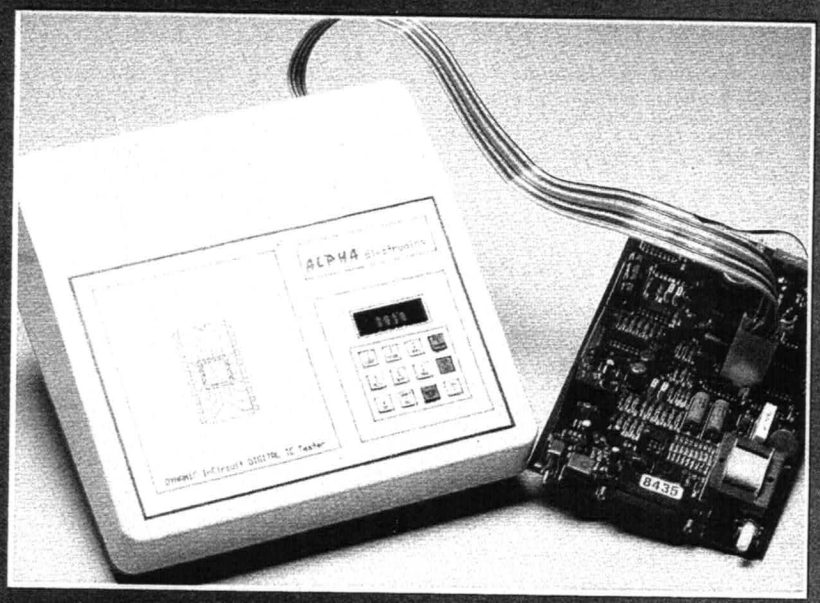
SMT SPECIAL 32-PAGE SECTION

$2.25 NOV. 1987
IN CANADA $2.75

TECHNOLOGY - VIDEO - STEREO - COMPUTERS - SERVICE

BUILD THIS COMPUTERIZED IC TESTER

Troubleshoot IC's in or out of circuit



THE TRUTH BEHIND THE BLUE BOX

And how Ma Bell crushed them

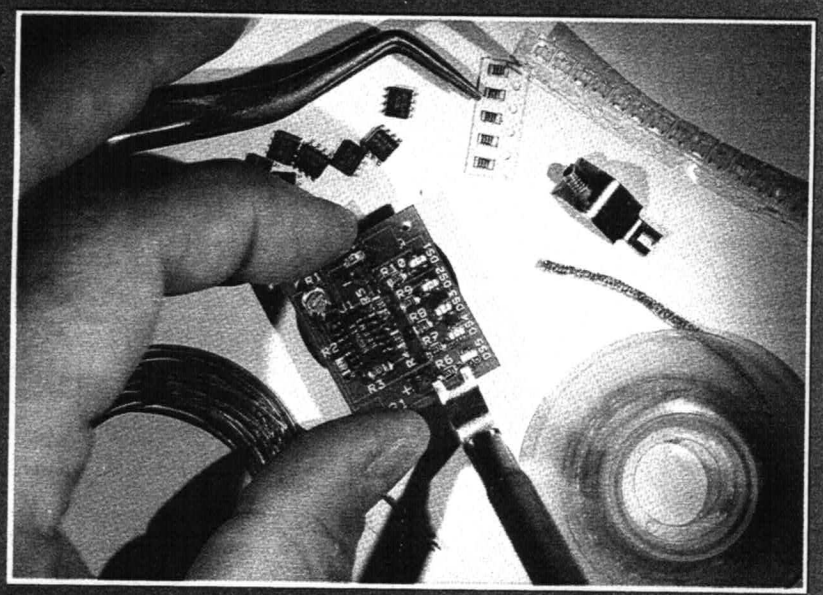
RF TRANSISTORS

Understanding the data sheets

A GERNSBACK PUBLICATION

SURFACE-MOUNT TECHNOLOGY

Forrest Mims brings you the technology and 4 projects you can build



COMPUTERDIGEST

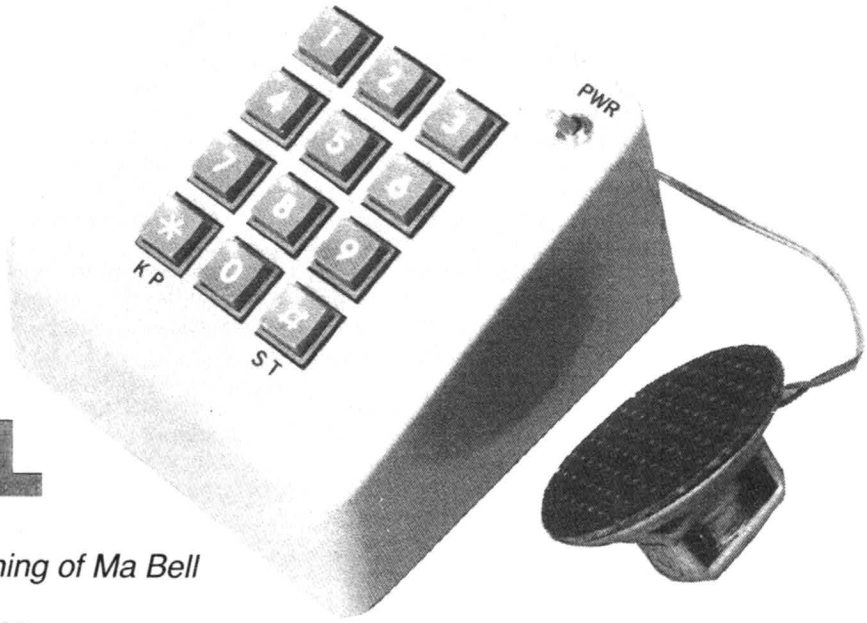
Turbocharging your PC

0 71896 48783 1 11

PLUS:

- ★ BUILD AN ELECTRONIC LOCK
- ★ POOR MAN'S STORAGE SCOPE
- ★ SEMICONDUCTOR TESTING

THE BLUE BOX AND MA BELL

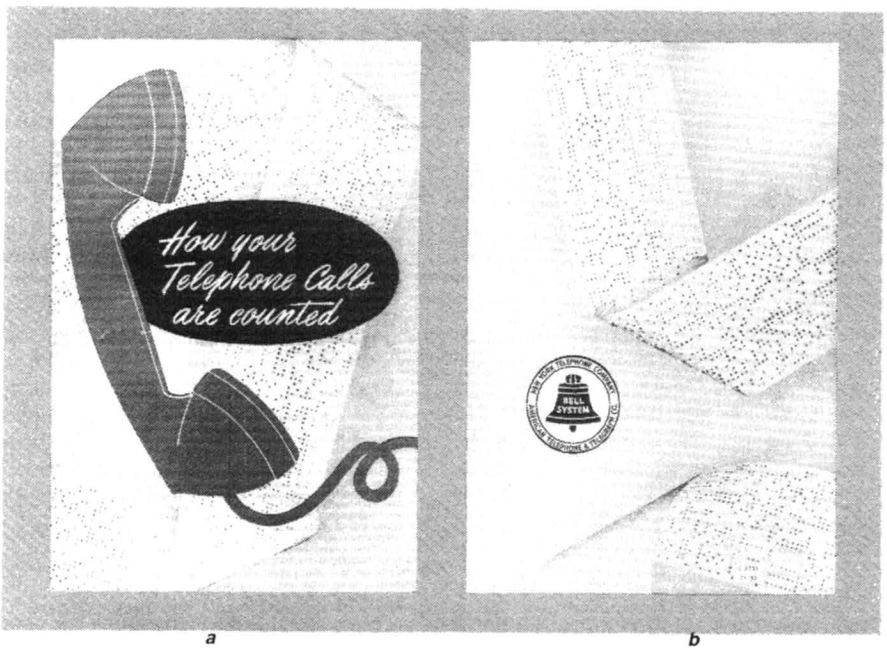


When blue and red meant the trashing of Ma Bell

HERB FRIEDMAN, COMMUNICATIONS EDITOR

BEFORE THE BREAKUP OF AT&T, MA BELL was everyone's favorite enemy. So it was not surprising that so many people worked so hard and so successfully at perfecting various means of making free and untraceable telephone calls. Whether it was a *Red Box* used by Joe and Jane College to call home, or a *Blue Box* used by organized crime to lay off untraceable bets, the technology that provided the finest telephone system in the world contained the seeds of its own destruction.

The fact of the matter is that the Blue Box was so effective at making untraceable calls that there is no estimate as to how many calls were made or who made them. No one knows for certain whether Ma Bell lost revenues of $100, $100-million, or $1-billion on the Blue Box. Blue Boxes were so effective at making free, untraceable calls that Ma Bell didn't want anyone to know about them, and for many years denied their existence. They even went as far as strong-arming a major consumer-science magazine into killing an article that had already been prepared on the Blue and Red boxes. Further, the police records of a major city contain a report concerning a break-in at the residence of the author of that article. The only item missing following the break-in was the folder containing copies of one of the earliest Blue-Box designs and a Bell-System booklet that described how subscriber billing was done by the AM[illegible]achine—a booklet that Ma Bell de[illegible]r existed; Fig. 1 proves otherwise. Since the AMA (*A*utomatic *M*essage *A*ccounting) machine was the means whereby Ma Bell eventually tracked down both the Blue and Red Boxes, we'll take time out to explain it. Besides, knowing how the AMA machine works will help you to better understand Blue and Red Box "phone phreaking."



a *b*

FIG. 1—THE BOOKLET THAT NEVER EXISTED. Although its existence was denied, the front (*a*) has a photograph of an AMA tape, while the back (*b*) has the Bell System logo.

Who made the call?

Back in the early days of the telephone, a customer's billing originated in a mechanical counting device, which was usually called a "register" or a "meter." Each subscriber's line was connected to a meter that was part of a wall of meters. The meter clicked off the message units, and once a month someone simply wrote down the meter's reading, which was later interpolated into message-unit billing for those subscriber's who were charged by the message unit. (Flat-rate subscriber's could make unlimited calls only within a designated geographic area. The meter clicked off message units for calls outside that area.) Because eventually there were too many meters to read individually, and because more subscribers started questioning their monthly bills, the local telephone companies turned to photography. A photograph of a large number of meters served as an incontestable record of their reading at a given date and time, and was much easier to convert to customer billing by the accounting department.

As you might imagine, even with photographs billing was cumbersome and did not reflect the latest technical developments. A meter didn't provide any indication of what the subscriber was doing with the telephone, nor did it indicate how the average subscriber made calls or the efficiency of the information service (how fast the operators could handle requests). So the meters were replaced by the AMA machine. One machine handled up to 20,000 subscribers. It produced a punched tape for a 24-hour period that showed, among other things, the time a phone was picked up (went off-hook), the number dialed, the time the called party answered, and the time the originating phone was hung up (placed on-hook).

One other point, which will answer some questions that you're certain to think of as we discuss the Red and Blue boxes: Ma Bell did not want persons outside their system to know about the AMA machine. The reason? Almost everyone had complaints—usually unjustified—about their billing. Had the public been aware of the AMA machine they would have asked for a monthly list of their telephone calls. It wasn't that Ma Bell feared errors in billing; rather, they were fearful of being buried under an avalanche of paperwork and customer complaints. Also, the public believed their telephone calls were personal and untraceable, and Ma Bell didn't want to admit that they knew about the who, when, and where of every call. And so Ma Bell always insisted that billing was based on a meter that simply "clicked" for each message unit; that there was no record, other than for long-distance calls, as to who called whom. Long distance was handled by, and the billing information was done by an operator, so there was a written record Ma Bell could not deny.

The secrecy surrounding the AMA machine was so pervasive that local, state, and even federal police were told that local calls made by criminals were untraceable, and that people who made obscene telephone calls could not be tracked down unless the person receiving the call could keep the caller on the line for some 30 to 50 minutes so the connections could be physically traced by technicians. Imagine asking a woman or child to put up with almost an hour's worth of the most horrendous obscenities in the hope someone could trace the line. Yet in areas where the AMA machine had replaced the meters, it would have been a simple, though perhaps time-consuming task, to track down the numbers called by any telephone during a 24-hour period. But Ma Bell wanted the AMA machine kept as secret as possible, and so many a criminal was not caught, and many a woman was harried by the obscene calls of a potential rapist, because existence of the AMA machine was denied.

As a sidelight as to the secrecy surrounding the AMA machine, someone at Ma Bell or the local operating company decided to put the squeeze on the author of the article on Blue Boxes, and reported to the Treasury Department that he was, in fact, manufacturing them for organized crime—the going rate in the mid 1960's was supposedly $20,000 a box. (Perhaps Ma Bell figured the author would get the obvious message: Forget about the Blue Box and the AMA machine or you'll spend lots of time, and much money on lawyer's fees to get out of the hassles it will cause.) The author was suddenly visited at his place of employment by a Treasury agent.

Fortunately, it took just a few minutes to convince the agent that the author was *really* just that, and not a technical wizard working for the mob. But one conversation led to another, and the Treasury agent was astounded to learn about the AMA machine. (Wow! Can an author whose story is squelched spill his guts.) According to the Treasury agent, his department had been told that it was impossible to get a record of local calls made by gangsters: The Treasury department had never been informed of the existence of automatic message accounting. Needless to say, the agent left with his own copy of the Bell System publication about the AMA machine, and the author had an appointment with the local Treasury-Bureau director to fill him in on the AMA machine. That information eventually ended up with Senator Dodd, who was conducting a congressional investigation into, among other things, telephone company surveillance of subscriber lines—which was a common practice for which there was detailed instructions, Ma Bell's own switching equipment ("crossbar") manual.

TABLE 1—CCITT NUMERICAL CODE

Digit	Frequencies (hz)	
1	700 + 900	
2	700 + 1100	
3	900 + 1100	
4	700 + 1300	
5	900 + 1300	
6	1100 + 1300	
7	700 + 1500	
8	900 + 1500	
9	1100 + 1500	
0	1300 + 1500	
Code 11	700 + 1700	FOR INWARD
Code 12	900 + 1700	OPERATORS
KP	1100 + 1700	PRIME (START OF PULSING)
KP2	1300 + 1700	TRANSIT TRAFFIC
ST	1500 + 1700	START (END OF PULSING)

The Blue Box

The Blue Box permitted free telephone calls because it used Ma Bell's own internal frequency-sensitive circuits. When direct long-distance dialing was introduced, the crossbar equipment knew a long-distance call was being dialed by the three-digit area code. The crossbar then converted the dial pulses to the CCITT tone groups, shown in Table 1, that are used for international and trunkline signaling. (Note that those do not correspond to *Touch-Tone* frequencies.) As you can see in that table, the tone groups represent more than just numbers; among other things there are tone groups identified as KP (*prime*) and ST (*start*)—keep them in mind.

When a subscriber dialed an area code and a telephone number on a rotary-dial telephone, the crossbar automatically connected the subscriber's telephone to a long-distance trunk, converted the dial pulses to CCITT tones, set up electronic cross-country signaling equipment, and recorded the originating number and the called number on the AMA machine. The CCITT tones sent out on the long-distance trunk lines activated special equipment that set up or selected the routing, and caused electro-mechanical equipment in the target city to dial the called telephone.

Operator-assisted long-distance calls worked the same way. The operator simply logged into a long-distance trunk and pushed the appropriate buttons, which generated the same tones as direct-dial equipment. The button sequence was KP (which activated the long-distance equipment), then the complete area code and telephone number. At the target city, the connection was made to the called number but ringing did not occur until the operator there pressed the ST button.

The sequence of events of early Blue Boxes went like this: The caller dialed information in a distant city, which caused his AMA machine to record a free call to information. When the information operator answered, he pressed the KP key on the Blue Box, which disconnected the operator and gave him access to a long-distance trunk. He then dialed the desired number and ended with an ST, which caused the target phone to ring. For as long as the conversation took place, the AMA machine indicated a free call to an information operator. The technique required a long-distance information operator because the local operator, not being on a long distance trunk, was accessed through local wire switching, not the CCITT tones.

Call anywhere

Now imagine the possibilities. Assume the Blue Box user was in Philadelphia. He would call Chicago information, discon-

nect from the operator with a KP tone, and then dial anywhere that was on direct-dial service: Los Angeles, Dallas, or anywhere in the world if the Blue Boxer could get the international codes.

The legend is often told of one Blue Boxer who, in the 1960's, lived in New York and had a girl friend at a college near Boston. Now back in the 1960's, making a telephone call to a college town on the weekend was even more difficult than it is today to make a call from New York to Florida on a reduced-rate holiday using one of the cut-rate long-distance carriers. So our Blue Boxer got on an international operator's circuit to Rome, Blue Boxed through to a Hamburg operator, and asked Hamburg to patch through to Boston. The Hamburg operator thought the call originated in Rome and inquired as to the "operator's" good English, to which the Blue Boxer replied that he was an expatriate hired to handle calls by American tourists back to their homeland. Every weekend, while the Northeast was strangled by reduced-rate long-distance calls, our Blue Boxer had no trouble sending his voice almost 7,000 miles for free.

Vacuum tubes

Assembly plans for Blue Boxes were sold through classified advertisements in the electronic-hobbyist magazines. One of the earliest designs was a two-tube portable model that used a 1.5-volt "A" battery for the filaments and a 125-volt "B" battery for the high-voltage (B+) power supply. The portable Blue Box's functional circuit is shown in Fig. 2. It consisted of two phase-shift oscillators sharing a common speaker that mixed the tones from both oscillators. Switches S1 and S2 each represent 12 switching circuits used to generate the tones. (*No, we will not supply a working circuit, so please don't write in and ask—Editor.)* The user placed the speaker over the telephone handset's transmitter and simply pressed the buttons that corresponded to the desired CCITT tones. It was just that simple.

Actually, it was even easier than it reads because Blue Boxers discovered they did not need the operator. If they dialed an active telephone located in certain nearby, but different, area codes, they could Blue Box just as if they had Blue Boxed through an information operator's circuit. The subscriber whose line was Blue Boxed simply found his phone was dead when it was picked up. But if the Blue Box conversation was short, the "dead" phone suddenly came to life the next time it was picked up. Using a list of "distant" numbers, a Blue Boxer would never hassle anyone enough time to make them complain to the telephone company.

The difference between Blue Boxing off of a subscriber rather than an information operator was that the Blue Boxer's AMA tape indicated a real long-distance telephone call—perhaps costing 15 or 25 cents—instead of a freebie. Of course, that is the reason why when Ma Bell finally decided to go public with "assisted" newspaper articles about the Blue Box users they had apprehended, it was usually about some college kid or "phone phreak." One never read of a mobster being caught. Greed and stupidity were the reasons why the kid's were caught.

It was the transistor that led to Ma Bell going public with the Blue Box. By using transistors and RC phase-shift networks for the oscillators, a portable Blue Box could be made inexpensively, and small enough to be to be used unobtrusively from a public telephone. The college crowd in many technical schools went crazy with the portable Blue Box; they could call the folks back home, their friends, or get on a free network (the Alberta and Carolina connections—which could be a topic for a whole separate article) and never pay a dime to Ma Bell.

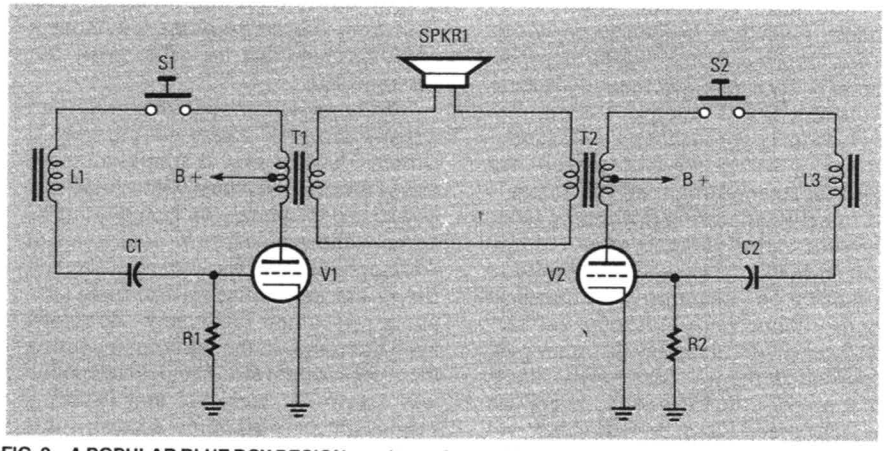


FIG. 2—A POPULAR BLUE BOX DESIGN used two phase-shift oscillators, vacuum tubes, and a simple speaker connection that mixed both oscillators into a single two-tone output.

Unlike the mobsters who were willing to pay a small long-distance charge when Blue Boxing, the kids wanted it, wanted it all free, and so they used the information operator routing, and would often talk "free-of-charge" for hours on end.

Ma Bell finally realized that Blue Boxing was costing them *Big Bucks*, and decided a few articles on the criminal penalties might scare the Blue Boxers enough to cease and desist. But who did Ma Bell catch? The college kids and the greedies. When Ma Bell decided to catch the Blue Boxers she simply examined the AMA tapes for calls to an information operator that were excessively long. No one talked to an operator for 5, 10, 30 minutes, or several hours. Once a long call to an operator appeared several times on an AMA tape, Ma Bell simply monitored the line and the Blue Boxer was caught. (Now do you understand why we opened with an explanation of the AMA machine?) If the Blue Boxer worked from a telephone booth, Ma Bell simply monitored the booth. Ma Bell might not have known who originated the call, but she did know who got the call, and getting that party to spill their guts was no problem.

The mob and a few Blue Box hobbyists (maybe even thousands) knew of the AMA machine, and so they used a real telephone number for the KP skip. Their AMA tapes looked perfectly legitimate. Even if Ma Bell had told the authorities they could provide a list of direct-dialed calls made by local mobsters, the AMA tapes would never show who was called through a Blue Box. For example, if a bookmaker in New York wanted to lay off some action in Chicago, he could make a legitimate call to a phone in New Jersey and then Blue Box to Chicago. His AMA tape would show a call to New Jersey. Nowhere would there be a record of the call to Chicago. Of course, automatic tone monitoring, computerized billing, and ESS (*E*lectronic *S*witching *S*ystems) now makes that all virtually impossible, but that's the way it was.

You might wonder how Ma Bell discovered the tricks of the Blue Boxers. Simple, they hired the perpetrators as consultants. While the initial newspaper articles detailed the potential jail penalties for apprehended Blue Boxers, except for Ma Bell employees who assisted a Blue Boxer, it is almost impossible to find an article on the resolution of the cases because most hobbyist Blue Boxers got suspended sentences and/or probation if they assisted Ma Bell in developing anti-Blue Box techniques. It is asserted, although it can't be easily proven, that cooperating ex-Blue Boxers were paid as consultants. (If you can't beat them, hire them to work for you.)

Should you get any ideas about Blue Boxing, keep in mind that modern switching equipment has the capacity to recognize unauthorized tones. It's the reason why a local office can leave their subscriber *Touch-Tone* circuits active, almost inviting you to use the *Touch-Tone*

service. A few days after you use an unauthorized *Touch-Tone* service, the business office will call and inquire whether you'd like to pay for the service or have it disconnected. The very same central-office equipment that knows you're using *Touch-Tone* frequencies knows if your line is originating CCITT signals.

The Red Box

The Red Box was primarily used by the college crowd to avoid charges when frequent calls were made between two particular locations, say the college and a student's home. Unlike the somewhat complex circuitry of a Blue Box, a Red Box was nothing more than a modified telephone; in some instances nothing more than a capacitor, a momentary switch, and a battery.

As you recall from our discussion of the Blue Box, a telephone circuit is really established before the target phone ever rings, and the circuit is capable of carrying an AC signal in either direction. When the caller hears the ringing in his or her handset, nothing is happening at the receiving end because the ringing signal he hears is really a tone generator at his local telephone office. The target (called) telephone actually gets its 20 pulses-per-second ringing voltage when the person who dialed hears nothing—in the "dead" spaces between hearing the ringing tone. When the called phone is answered and taken off hook, the telephone completes a local-office DC loop that is the signal to stop the ringing voltage. About three seconds later the DC loop results in a signal being sent all the way back to the caller's AMA machine that the called telephone was answered. Keep that three-second AMA delay in mind. (By now you should have a pretty good idea of what's coming!)

Figure 3 shows the simplified functional schematic of a telephone. Switch S1 is the hook switch. When S1 is open (on-hook) only the ringer circuit consisting of C1 and BELL1 is connected across the line. Capacitor C1 really has no purpose in the ringing circuit; it only serves to keep DC from flowing through BELL1. When the local telephone office feeds a 20-pps ringing signal into the line it flows through C1 and a ringer coil in BELL1. A vibrating device attached to BELL1 strikes a small bell—the ringing device. When the phone is answered by lifting the handset from its cradle, switch S1 closes (goes off-hook) and connects the handset across the telephone line. Since the handset's receiver and transmitter (microphone) are connected in series, a DC path is established from one side of the line to the other—what is called completing a DC loop with the central office. The DC current flowing in the loop causes the central office to instantly stop the ringing signal. When the handset is replaced in its cradle, S1 is opened, the DC loop is broken, the circuit is cleared, and a signal is sent to the *originating* telephone's AMA machine that the called party has disconnected.

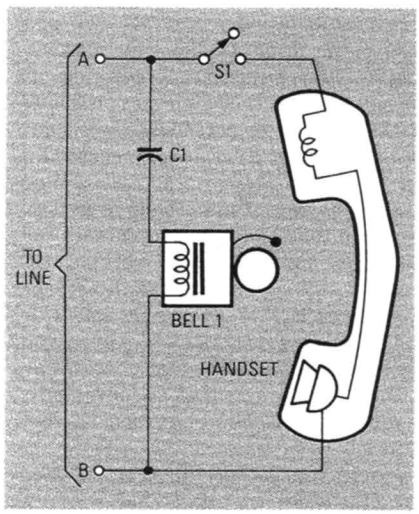


FIG. 3—A SIMPLIFIED TELEPHONE circuit. The handset is connected across the line when hook switch S1 is closed. The handset closes the DC loop with the telephone company's switching equipment.

Now as we said earlier, the circuit can actually carry AC before the DC loop is closed. The Red Box is simply a device that provides a telephone with a local battery so that the phone can generate an AC signal without having a DC connection to the telephone line. The earliest of the Red Boxes was the surplus military field telephone, of which there were thousands upon thousands in the marketplace during the 1950's and 1960's, The field telephone was a portable telephone unit having a manual ringer worked by a crank—just like the telephone Grandpa used on the farm—and two D-cells. A selector switch set up the unit so that it functioned as a standard telephone that could be connected to a combat switchboard, with the DC power supplied by the switchboard. But if a combat unit wasn't connected to a switchboard, and the Lieutenant yelled "Take a wire," the signalman threw a switch on his field telephone that switched in the local batteries. To prevent the possibility of having both ends of the circuit feeding battery current into the line in opposite polarity—thereby resulting in silence—the output from the field telephone when running from its internal batteries was only the AC representing the voice input, not modulated DC.

Figure 4 is the functional simplified schematic for a field telephone (**do not attempt to build that circuit**). Momentary switch S4 is not part of the field telephone, it is added when the phone is converted to a Red Box; so for now, consider that S4 does not exist. Once again, S1 is the hook switch. When S2 is set to N (NORMAL) and S1 is closed, DC flows from line A through T1's secondary (S),

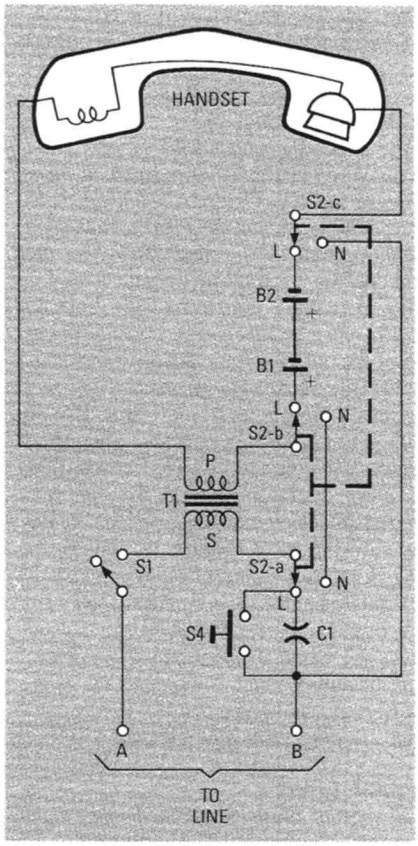


FIG. 4—A SIMPLIFIED RED BOX. Switch S2 lifts the handset from the telephone line and connects two D-cells as a local power supply. The circuit is DC-isolated from the telephone line even when hook switch S1 is closed.

through S2-a to S2-b, through T1's primary (P), through the handset, through S2-c, to line B. There is a complete DC path across the line, and if the unit is connected across a conventional subscriber telephone line it will close the DC loop from the local office.

To use the field telephone as a Red Box, switch S2 is set to L (LOCAL). Switches S2-b and S2-c connect batteries B1 and B2 in series with the handset and the transformer's primary, which constitute an active, working telephone circuit. Switch S2-a connects T2's secondary to one side of the telephone line through a non-polarized capacitor (C1), so that when hook-switch S1 is closed, T1's secondary cannot close the DC loop.

Press once to talk

The Red Box was used at the receiving end; let's assume it's the old homestead. The call was originated by Junior (or Sis) at their college 1000 miles from home. Joe gave the family one ring and then hung up, which told them that he's calling. Pop set up the Red Box by setting S2 to LOCAL. Then Junior redialed the old homestead. Pop lifted the handset when the phone rang, which closed S1. Then Pop closed momentary-switch S4 for about a half-second, which caused the local telephone

continued on page 129

BLUE BOX

continued from page 52

office to silence the ringing signal. When Pop released S4, the folks can talk to Junior without Junior getting charged because his AMA tape did not show his call was answered—the DC loop must be closed for at least three-seconds for the AMA tape to show Junior's call was answered. All the AMA tape showed is that Junior let the phone ring at the old homestead for almost 30 minutes; a length of time that no Bell Operating Company is likely to believe twice!

A modern Red Box is simply a conventional telephone that's been modified to emulate the vintage 1940 military field telephone. Aside from the fact that the operating companies can now nail every Red Box user because all modern billing equipment shows the AMA information concerning the length of time a caller let the target telephone ring, it's use has often put severe psychological strain on the users.

Does getting electronics mixed up with psychology sound strange? Well it isn't because it's what helped Ma Bell put an end to indiscriminate use of the Red Box. The heyday of the Red Box was the 1950's and 1960's. Mom and Pop were lucky to have finished high school, and almost without exception, both elementary and high schools taught honesty and ethics. Mom and Pop didn't have the chance to take college courses in *Stealing 101* that masqueraded under quaint names such as *Business Management*, *Marketing*, or *Arbitrage*. When Junior tried to get the old folks to use his "free telephone" they just wouldn't go along. So Junior installed the Red Box at his end. He gave one ring to notify the family to call back. When Pop called Junior, it was Junior who was using the Red Box. Problem was, Junior didn't know that the AMA tape for Mom and Pop's phone showed a 20- or 30-minute ringing. When Ma Bell's investigators showed up it was at the old homestead; and it was only then that the folks discovered their pride and joy had been taught to steal.

There are no hard facts concerning how many Red Boxes were in use, or how much money Ma Bell lost, but one thing is known: she had little difficulty is closing down Red Boxes in virtually all instances where the old folks were involved because Mom and Pop usually would not tolerate what to them was *stealing*. If you as a reader have any ideas about using a Red Box, bear in mind that the AMA (or its equivalent) will get you every time, even if you use a phone booth, because the record will show the number being called, and as with the Blue Box, the people on the receiving end will spill their guts to the cops. **R-E**

ELECTRONIC LOCK

continued from page 108

one for the common signal and electrical ground.

Build the encoder circuit on a small, piece of perforated wiring board, and, if possible, use a socket for IC2, because being a CMOS device, it can be damaged if you solder directly to its terminals, especially if you're using an ungrounded soldering iron. For the same reason, use a socket for the decoder's IC1.

As shown in Fig. 3, the small encoder assembly can be secured directly to one side of a DB-25-type connector hood using two 4-40 screws.

Testing

Testing is very simple. Connecting the key to the decoder should cause RY1's contacts to close. If the contacts don't close, it's more than likely the problem is an address mismatch between encoder and decoder. Check that they are exactly the same. If you connect an oscilloscope to pin 15 of IC2 should see a constant sequence of pulses being transmitted out of the encoder. If the pulses are missing check that resistors R4 and R5, and capacitor C3, are connected correctly. **R-E**