

PHONE COLOR BOXES

COPYRIGHT © 1986, JOHN J. WILLIAMS and FAMILY. ABSOLUTELY ALL RIGHTS RESERVED
By: John J. Williams, MSEE --- CONSUMERTRONICS CO., P.O. Drawer 537, Alamogordo, NM 88310

PHONE PHREAKING

Phone color boxes were not only one of the most outstanding and publicized features of the 1960s Hippie-Yippie movement, but are fascinating to many "straight" people even today. You can thank Bell for most of this fascination because Bell turned itself into a huge, highly secretive organization that permeates everyone's existence. Penetrating its deepest secrets was tantamount to a free pass to the land of Oz. Defeating the clutching grasps of the goons it employs to protect its security was tantamount to out-jousting the black knight. To many, it was such an exhilarating challenge that they would spend enormous parts of their lives dedicated to the quest.

The term "Bell" is used here as a generalized phone company name and is NOT an abbreviation of any specific local or Long Distance phone company. I prefer the term "Bell" over "Teleco," and "Bell" is used in honor of the inventor of the telephone. The use of phone color boxes to obtain free or low cost phone calls is known as "phreaking" (PHREAK = PHone fREAK) or "phone boxing."

Phreaking hit its peak in the 1960s with the advent of some of its most colorful and legendary characters (Capt. Crunch, Abbie Hoffman, Cheshire Cat, etc.), and the Yippie publishing enterprise known as TAP. For more historical information on phreaking, see, "SECRETS OF THE LITTLE BLUE BOX", ESQUIRE, Oct. 1971, and "THE FIRST COMPUTER FREAKS", ESQUIRE, June, 1983.

The phone boxing movement went thru two step-down periods and one step-up period. The first step-down period came in the early 1970s when many of the groupies and me-tooers of the spirited sixties movements drifted into conventional lifestyles. In fact, about 90% of the self-proclaimed hippies and yuppies of the early '60s turned legit by 1976. This also resulted in much lessened publicity for the movement and their outrageous activities.

The second step-down period started about 1978. Many of the remaining hard-core phreakers turned to microcomputing. Radio Shack, Apple and Commodore came out with their primitive prototypes. They were great hardware and software challenges, and, in those early days, their modems were in little use and also primitive. It took some time for phreakers to move up the learning curve sufficiently enough, and for the development of more sophisticated computers and modems, before attention was again seriously turned to phreaking.

There was also the factor that Bell developed sophisticated countermeasures to stop three of the most costly phone boxes, the red, blue and black boxes. Many carefree phreakers soon found their asses in jail charged with such things as "theft of service" and "possession of burglary tools" (color boxes). Phreakers got so paranoid that they would only operate from payphones, college dormitories, or other facilities where pinpointing the culprit was difficult at best - then only for short periods of time!

The advent of ESS over the old-style crossbar switching techniques gave Bell awesome powers to quickly detect and apprehend phreakers. With ESS, Bell could automatically scan thousands of phone lines for cheating, and, once cheating was discovered, could automatically print out both origin and destination phone numbers, names and locations within seconds.

The step-up in phreaking started in about 1980. The phreakers were then prepared to engage in computer wars with Bell or anyone else they wanted to mess with. Phreaking then metamorphosed into far more diverse and complex sorts of cheating, madness and mayhem. No longer was it primarily an adolescent game although most of the CAUGHT phreakers were quite young - some preteen! No longer were phreakers content in just beating Bell and getting free calls. Now, they went for the jugular! With new and powerful capabilities that governments, phone companies, corporations and institutions were slow to counteract, phreakers penetrated large computer systems. In the process, they ripped-off \$ Billions, destroyed businesses, compromised national secrets, etc. That's not to say that all or even most computer phreaking was vicious or harmful - most was not. See our COMPUTER PHREAKING (\$15) for more information on computer phreaking.

Lost in all the computer phreaking smoke was the continued and increasing phone phreaking efforts. Phone phreaking increased because of these reasons:

(1) Color box phreakers were coming up with new boxes, new circuits and new techniques to beat Bell's countermeasures. Small microcomputers, particularly the TI-99/4A were adapted to perform as color boxes. Sophisticated software techniques were developed. The view of the law here is clear. If one is caught with a device solely dedicated to robbing Bell, he can be charged for "possession of burglary tools." However, if one is caught with a small computer that has countless legal applications, unless it can be clearly shown that the computer is used for phreaking (ex: caught in the act), then police authorities cannot LEGALLY charge a person with "possession of burglary tools" for possessing a computer.

(2) The break-up of AT&T lead to real or imagined decreases in Bell security. In fact, new phreaking techniques have been developed that take advantage in differences between AT&T, MCI, SPRINT, and others.

(3) The advent of the phone credit card opened up a goldmine for phreakers. The only obstacle was discovering viable credit card numbers. At one time, Bell handed out phone credit cards like candy. Getting valid numbers was no problem - and still is no problem! Despite dedicated FBI efforts to stop Bulletin Boards (BBS) from publishing these numbers, many still do either inadvertently or purposefully. \$ Billions have been stolen from Bell just due to their stupidity of issuing phone credit cards!

Unfortunately, TAP did not survive far into this upswing. In mid-1984, after publishing 92 issues, TAP was put out of business. From the best information we have, TAP was apparently penetrated by the combined forces of the FBI and Bell, its subscription lists compromised, and its headquarters set on fire as a cover up. Membership scattered. The problem with TAP was that it was a wide-open organization, mostly of former hippies and yuppies, and left itself vulnerable to penetration. Although TAP operated on the bare edges of illegality, apparently above-board legal action could not be brought against it. We all have the right to Freedom of Press - just as long as we don't offend any big-shots!

We have heard that TAP will begin publishing again in the near future, and that they will publish a book on, "The Best Of TAP." We don't know anything specific about where, when, how and how much. We are working on verification. When verified, we will let you know, provided that you supply us with a #10 SASE.

We have all 92 issues of this uncopyrighted publication. Although TAP was about 75% devoted to phone phreaking, it described many other technological defeats from ATMs to weapons. The left-wing slant in many of its articles did offend our conservative tastes. However, for its sheer gaul and detail of technological defeats, it was a real inspiration and one of several of our best sources for the survival information that CONSUMERTRONICS CO. publishes. We will sell you TAP back issue copies for \$2 each, or a copy of all TAP issues for \$150. Sorry, we have no index of back issues.

But all is not lost! Just before TAP was assassinated, on Jan. 1984, 2600 was born. 2600 is published by 2600 ENTERPRISES, P.O. Box 762, Middle Island, NY 11953. It's two BBS numbers are 201-366-4431 and 516-751-2600. 2600 is sort of the yuppie version of TAP. On one hand, 2600 is not as explicit as TAP and contains very few plans and schematics, and it is not as funky. On the other hand, 2600 is better organized, better formatted, is much easier to read, and has substantially more information.

2600 is also totally dedicated to phone and computer technology and phreaking, as opposed to other forms of phreaking and to survivalism in general. From our point of view and that of about 90% of our readers, because of 2600's lack of general survival information and how-to-do plans, and the many other forms of creating mischief, mayhem and madness, 2600 is a poor replacement for TAP. But, from the point of view of readers who are focused into phone and computer phreaking, 2600 is a good replacement for TAP and improves upon TAP in many respects. Be as it may, CONSUMERTRONICS CO. will continue publishing its 70+ hardhitting how-to-do publications on virtually every form of survivalism and technological defeats. WE ARE ALWAYS AT YOUR SERVICE!

One publication that we advise that you AVOID is COMPUTEL, 6354 Van Nuys Blvd., No. 161, Van Nuys, CA 91401. COMPUTEL spent about \$100K over a two year period placing its display ads in national electronics and computer magazines. The display ads promised that for \$14, you would receive a year's subscription to their phreaker newsletter. We did. So did a number of our readers. To

our knowledge, no newsletter was ever published. It appears that some of their subscribers did complain to the Postal Inspector and to the magazines, but none, to our knowledge, ever received so much as a reply from them to any complaint against COMPUTEL, or a refund. Apparently, COMPUTEL was allowed to continue its ads in spite of complaints against it to the magazines! Although we have NO PROOF, we suspect that COMPUTEL is an FBI or police scam used to produce mailing lists of people interested in phreaking, and to get phreaking pros to submit articles to learn of new techniques. They asked us to submit articles. If you know anything about COMPUTEL, please send to us and to 2600.

WAVESHAPES

Most phone color boxes require the generation of certain waveforms to accomplish their purposes. The pulses that make up these waveforms can take on a number of waveshapes. The various possible waveshapes are:

(A) **SQUARE WAVE:** Square waves are the easiest to generate using digital circuits. Unfortunately, they are rich in higher frequency harmonics, sound harsh and are thus more risky to use. The risk in using square waves largely depends upon the method of coupling into the phone circuit. If a direct, electrical coupling is made, although the 3000 Hz cutoff frequency of most phone circuits will tend to do some smoothing, it won't do enough to make a big difference. If coupling is made by holding the box speaker to the phone mouthpiece (acoustical coupling) or by inductive coupling, filtering will be substantial and the resultant waveshape will approximate a sine wave. Although most phreakers prefer to acoustically couple using ripped-off payphone earpieces, one can purchase an excellent inductive coupler from TRINETICS INC., 55807 Currant Rd., Mishawaka, IN 46544.

(B) **HF FILTERED SQUARE WAVE:** Filtering out the high frequency harmonics from a square wave produces a shark-tooth wave. Not normally used for boxing.

(C) **TRIANGLE WAVE:** A triangle wave can be generated by the Signetics 566, EXAR XR-2240 and other oscillator chips. Still

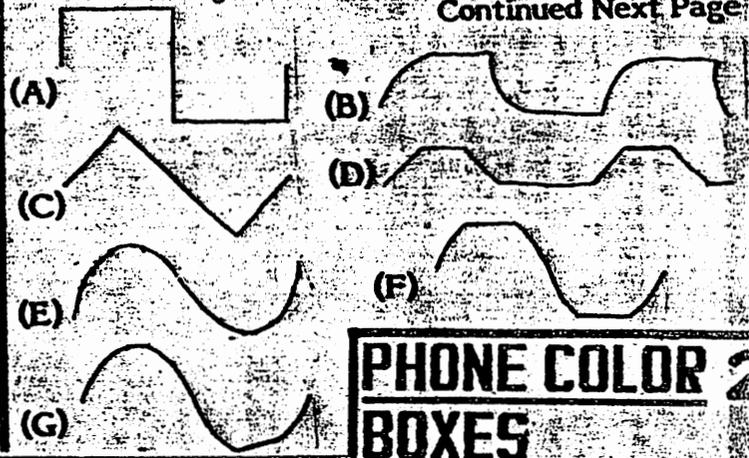
plagued with higher frequency harmonics, it is better than a square wave but worse than a sine wave.

(D) **TRAPEZOIDAL WAVE:** A trapezoidal wave can be generated by clipping a triangle wave. In modern MF equipment, trapezoidal waves are used because they are harder to generate. Thus, trapezoidal waves are preferred for Blue Boxing.

(E) **SINEWAVE:** Generated from analog equipment, the sine wave has no harmonics and, before the advent of trapezoidal MF tones, was the preferred waveform for all forms of boxing.

(F) **CLIPPED SINEWAVE:** The clipped-sine wave closely resembles the trapezoidal wave, and works as well.

(G) **TWIN-T OSCILLATOR WAVE:** The twin-T wave closely resembles the sine wave (some slight distortion), and is as good as the sine wave for boxing.



QUALIFICATIONS & INFO.

Although every reasonable effort has been made to provide complete and accurate information, we do not assume liability for any losses or damages whatsoever, either direct or consequential, for any errors or omissions found herein. **PHONE COLOR BOXES** is sold, 'as is', and for **EDUCATIONAL PURPOSES ONLY**. We do NOT recommend or suggest that illegal devices of any kind be actually applied to any phone equipment at any time.

If you find any errors or omissions, please let us know. **CONSUMERTRONICS CO.** is known as **THE NATIONAL CLEARINGHOUSE FOR SURVIVAL INFORMATION**. **PHONE COLOR BOXES** (as well as most of our other publications) has benefited from substantial informational contributions - mostly from TAP and 2600. We thank all of these fine publications for the privilege of liberally quoting and excerpting from their fine publications.

If you have important, new, hard-to-find, invaluable, and/or shocking survival information of any type, please send it to us for our review. We are particularly interested in innovative computer security techniques - particularly dealing with ATMs and Credit Cards, and improvements on the security techniques found. If your information is new and substantial, we are interested in publishing it in the future, and you want compensation for it, we will negotiate with you for the rights to publish your information. Please send us all of the information you have for our review, to the address below. If compensation is desired, please specify that intent in your cover letter.

Due to lack of staff, we cannot provide advice to solve complex individual problems. For all inquiries, please send us a letter/note, and enclose a #10 SASE. Please do not phone. If we are able to help you, we will respond.

We are available as security and survival consultants for a fee. Please send us a complete description of your problem, and \$25. We will perform a preliminary analysis of your problem for you, and provide you an estimate. We guarantee total confidentiality. We can handle virtually any problem relating to security and survival from software development to searches of any kind.

We publish 70+ survival publications on energy, weapons, security, computers, electronics, financial and medical. Along the same vein as **PHONE COLOR BOXES**, we also publish **TONE DEAF** (\$7), **VOICE DISGUISE** (\$7), **TELEPHONE RECORDER INTERFACE** (\$7), **COMPUTER PHREAKING** (\$15), **ABSOLUTE COMPUTER FILE SECURITY** (\$25) and **CRYPTANALYSIS TECHNIQUES** (\$25). Please send \$1 for our **SUPER-SURVIVAL CATALOG** (free with \$10+ order) to: **CONSUMERTRONICS CO.**, P.O. Drawer 537, Alamogordo, NM 88310.

TELECO SECURITY & AGENTS

Years ago, you paid a surprise visit on us because you claimed that our **TONE DEAF** publication information was being used by phone phreaks to rob the phone company. Although your visit provided clear proof that our methods work, your visit was obviously an attempt to intimidate us into ceasing publication. Be advised that we have the right to publish everything you find herein under our First Amendment rights. If you are not convinced of that fact by now, I can only suggest that you fire the shysters you employ and hire competent attorneys.

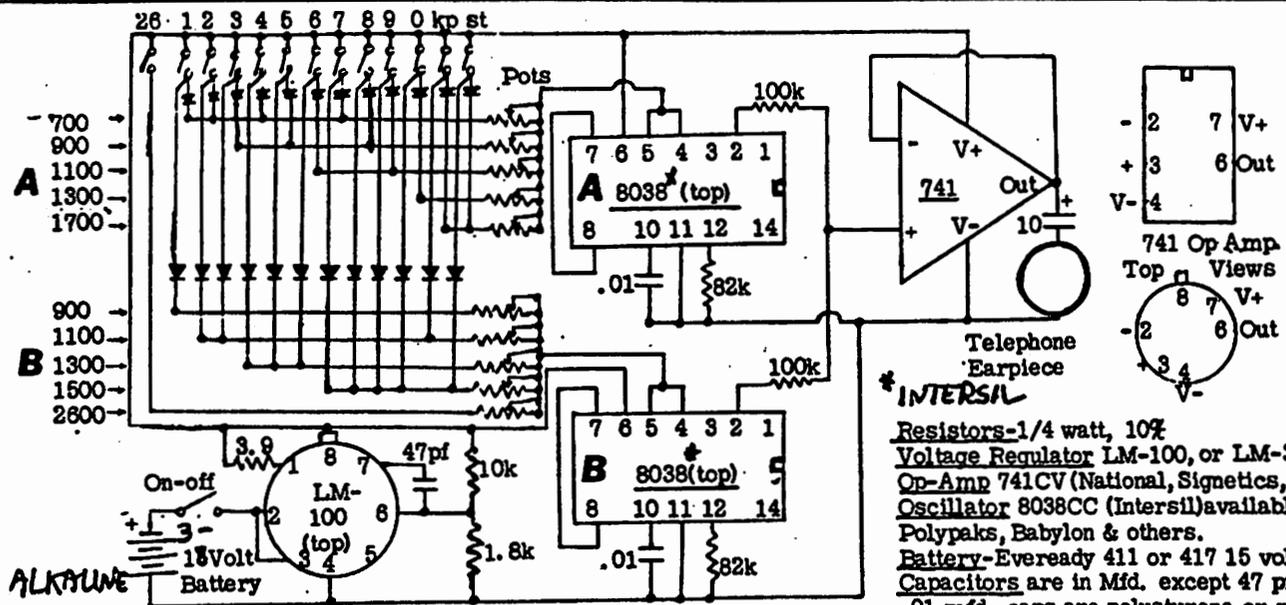
Further, be advised that if you wish to visit us again concerning **PHONE COLOR BOXES**, **TONE DEAF**, and/or any of our other publications, we will charge you \$1,000.00 per hour for our valuable time. The time will include preparing for your visit, your visit, and any action that we feel that your visit either directly or indirectly requires us to take. Any part of an hour will count as a full hour. We also require that you:

- (1) Schedule your visit with us at least 10 calendar days in advance, in writing.
- (2) Describe to us the exact nature and scope of your visit, in writing.
- (3) Provide us with identities of all of your people who will visit us, including their office positions, addresses and phone numbers, and the names of their immediate supervisors, in writing.
- (4) Accompany your schedule letter with a valid check made out to **CONSUMERTRONICS CO.** for at least \$10,000.00 towards covering resulting charges.
- (5) Agree that none of your personnel will carry any kind of weapon, recording device or radio transmitter with them for this visit.
- (6) Agree, in full, and in writing, to cover ALL of our legal expenses resulting from any kind of civil action brought by you and/or by us in which your visit is referred to in testimony.

If any of the above (1)-(6) requirements are not fully agreed upon and honored by you for any visit, we will charge you \$10,000.00 per hour for our time (same basis of calculation as above), and the provisions of (6) will automatically go into effect as if you had agreed with (6).

Whatever unpaid balance remains outstanding will accrue an interest of 1.5% per month. To "visit" means to visit any of us at any time inside or outside of our home, or to visit our home when unoccupied.

Finally, be advised that should at any time your personnel appear life threatening or to endanger our property, we shall take whatever non-violent and/or violent measures be required to neutralize your actions. **TO AVOID AN UNFORTUNATE MISUNDERSTANDING, NEVER APPROACH US UNSCHEDULED OR IN ANY KIND OF THREATENING, SHOCKING, SNEAKY OR SURPRISING MANNER!!**



- RESISTORS**-1/4 watt, 10%
Voltage Regulator LM-100, or LM-300
Op-Amp 741CV (National, Signetics, etc.)
Oscillator 8038CC (Intersil) available from Polypaks, Babylon & others.
Battery-Eveready 411 or 417 15 volt.
Capacitors are in Mfd. except 47 pf.
 .01 mfd. caps are polystyrene or mylar.
 All capacitors are 15 volts or greater.
Diodes-small-signal matched germanium, or silicon.
Pots-25k, 10 or 20 turn trimmers.

NEW BLUE BOX

As stated earlier, Blue Boxes are used to obtain free LD phone calls by manipulating MF signaling. The most popular Blue Box circuit we've been able to find is the "New Blue Box." The Intersil 8038CC Function Generator is the basis of this MF generator. By varying the external resistor, we change the frequency of the 8038. Distortion is about 1%. The diodes route the power supply voltage for different tones. Double-pole switches are available, and they eliminate the need for the diodes.

Quiescent current is about 45 ma (mainly due to the 8038s), so power is kept OFF until the box is used. Tuning is easy. One plugs in #1 8038 in the #1 socket, and fine-tunes the #1 bank of frequencies. The #1 8038 is then removed, and the #2 8038 is installed in the #2 socket. Frequencies of bank #2 are then fine-tuned. After all frequencies are set, one plugs in both 8038s and is ready to go.

SOME PHONE BASICS

There are two basic ways of dialing a phone: (1) Rotary dial. (2) Touch-Tone. Aside from the two electronic methods used to translate your dialing efforts into actual numbers, there is no difference in the effects that they have on the phone system.

There are two basic types of telephone offices thru which all calls are switched. The first is the Central Office (CO). The wires from your telephone go to your local CO. From there, if your call is a local call, it is switched to the destination phone if served by the same CO, else to another local CO that serves the destination phone then to the destination phone. The three-digit call prefix designates the CO that serves the destination phone. More than one CO can occupy the same building. The number of COs in your community is equal to the number of three-digit prefixes your local Bell serves.

For LD calls, your call is switched to a Toll Office (TO). The TO connects distant COs to each other. Most COs have a Centralized Automatic Message Accounting (CAMA) system. The CAMA equipment records your number, the date and time, the destination number, and the duration of the call (after call completion). This is used for billing purposes.

The CO relays the LD number to the TO. The TO contains a sender, which sends by whatever route is easiest a series of Multi-Frequency (MF) pulses to another TO in the area that you called according to the area code dialed. These pulses are picked up by the sender in the distal TO, which translates the three-digit prefix and connects you to the CO dialed. This CO then translates the remaining digits of the phone number and connects you to the line you dialed.

When the destination phone is answered, a signal is returned all the way down the line to your local CO to say that the call was completed. Then, when either you or your friend ("phriend") hang up, another signal is sent to your local CO to say that your call was completed. CAMA then sends all this information to the billing office. Since AT&T broke up, LD calls are billed by your LD Bell billing office, and local calls by your local Bell billing office.

One other thing about phones, the terms "tip" and "ring" are old terms that relate to the tip and sleeve of phone plugs. Just remember that "tip" refers to the green wire, while "ring" refers to the red wire.

CONSTRUCTION HINTS

The easiest means of prototype construction is with wirewrap on perforated board. Mistakes can be easily corrected, modifications can be easily made, and construction can be done compactly. The trim pots shown in these schematics should be 10- or 20-turn CER-MET pots. Avoid wirewound pots - they are too temperature sensitive. Don't try to skimp by using single-turn pots or one trim pot to serve all frequencies as fine tuning and insensitivity to vibration are critical. All resistors should be metal-film (not carbon), because metal-film resistors have better temperature stability. Capacitors shown in pf should be polystyrene if at all possible. The banded end is the negative end. If not polystyrene, use mylar or mica capacitors wherever possible.

Most of these designs require CMOS IC, because CMOS draws far less current than TTL, and CMOS can be operated over a much greater voltage range. CMOS circuits are static-sensitive. One should ground himself to earth ground thru a 1.0 Meg resistor (NEVER DIRECTLY CONNECT YOURSELF TO GROUND). All inputs to any CMOS device MUST BE CONNECTED - to an input, to ground or to +V. Any non-terminated inputs will cause circuit malfunction. All outputs need not be connected.

It may seem silly to use a voltage regulator with battery power, but CMOS oscillator frequencies, and some other components, are sensitive to voltage level and tone frequency stability is critical. If one uses fresh alkaline batteries only, he can get away without voltage regulation. Else, voltage regulation must be used.

We also strongly recommend using sockets for two reasons:

- (1) They make fine-tuning and repairs much easier.
- (2) Between box applications, one should pop some of the ICs out of their sockets to prevent unauthorized people from using the box and-or making hostile accusations based upon circuit design.

THE MENACE OF ESS

Electronic Switching System (ESS) is definitely the future wave in the Bell systems! The "Electronic" really stands for "Computer-Controlled." It is a menace to not only phone and computer phreakers but to all citizens. With ESS, Bell will have total computerized control of YOUR phone lines! Not only will Bell have a record of every LD call you make, but of every local and "free" call. And with massive computer memories, tremendous speeds and voice recognition technology, the future portends that Bell may also soon have a digitized recording of all actual conversations made by phone - recallable within seconds to any hooked-up computer terminal or printer anywhere in the world!

Consumertronics Co.

2011 CRESCENT DR., P. O. DRIVE 537,
ALAMOGORDO, NM 88310

Continued Next Page

As it is, at least four Government agencies, plus the Soviets and perhaps a few other countries, can scan most of the country's microwave phone transmissions to pick out conversations based upon certain words and phrases spoken during them. For example, if you responded to a question from your Mom with, "I'll kill time by watching President Jones...", the "kill" and the "President" could trigger a Government computer to lock in on and then record your entire conversation and create computerized files on you (and your Mom) - files that would automatically be transmitted to Government intelligence agency computer systems under terrorist headings. And you wouldn't even know about it! Your file could then get mixed up with that of a real terrorist, and transmitted to thousands of law enforcement entities. Before you know it, a Swat team is butchering you and your kids!! It doesn't take much imagination to figure out how gravely dangerous this situation is rapidly becoming!!

One of our most popular publications is the VOICE DISGUISER (\$7). It's clear that many Americans are waking up to this menace! PHONE LINES ARE NOT PRIVATE - USE YOUR HOME PHONE TO THE BARE MINIMUM - NEVER FULLY IDENTIFY YOURSELF OVER THE PHONE - NEVER SAY ANYTHING CONTROVERSIAL, SUBJECT TO MISUNDERSTANDING OR IN JEST - NEVER USE WORDS LIKE "KILL," "ROB," "DRUGS," ETC. - USE A VOICE DISGUISER IF AT ALL POSSIBLE!! Paranoia is fear over an imaginary menace. This menace is real and today! And don't phone us - always write.

Since ESS can record every key that you press, it will also record every foreign tone that you "play" over the phone. If you decide to entertain your Aunt Mildred from Marfa, TX, with your rendition of Mozart, send her a cassette tape by mail!

ESS also permits immediate call tracing. For example, if you were to place an anonymous tip to your local police, all they have to do is tap a button on their console, and presto!, within three seconds, they have your name, address and phone number on a CRT or printer! Long gone are the days when some hapless servant of Bell had to rush up and down mainframes to record activated steppers! Long gone are the days that your private call was hidden among the tons of wires hiding other people's calls! Long gone are the days that a pennyless, free-spirited hippy could call home to Mom from the corner payphone.

ESS will make placing phone calls much faster, will cut down enormously on fraudulent calls, will permit direct dialing overseas, and will provide a myriad of other nice phone conveniences. But ESS can be too easily corrupted and abused by those in power, and like creating super humans from recombinant DNA experiments, this technology is just too risky to our privacy and freedom. NOT ALL TECHNOLOGY IS GOOD, AND THERE IS NO MAJOR TECHNOLOGY EVER INVENTED THAT WAS EITHER FREE FROM CORRUPTION OR FREE FROM DEFEATS!

PHONE COLOR BOXES

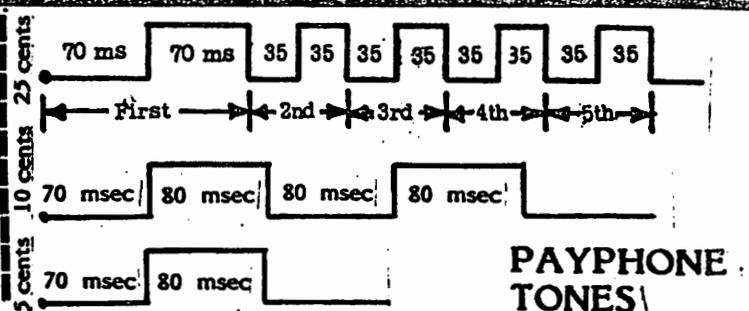
The four major phone color boxes are the Red, Blue, Black, and CF Box:

RED BOX

The Red Box is an electronic device that mimics the pulsed beeps produced in payphones ("fortress phones") when one drops coins into it to make a phone call. The objective is to make free payphone calls. The Red Box may be an electronic oscillator that produces the right tones, or a high-grade taperecorder in which previously recorded tones are played back. For recording, the taperecorder is connected directly to the phone line to record the coin sounds - not acoustically coupled. A phreaker calls from a payphone. When the phreaker answers, the phreaker deposits coins into the phone while the phreaker records the beeps. The phreaker can't hear the beeps because the earpiece is muted during coin deposits. Later, the phreaker plays back these sounds to simulate his own coin deposits. Note, that Red Boxes only work on single-coin-slot payphones - not on the old ones that have three round coin slots at the top.

The tones' intervals are not generated by the coins pushing levers on the payphone mechanism as most people believe, but by a small relay which reverses the direction of the wheel that the levers cock. In other words, when a coin is dropped by the operator, it pushes a plastic vane lever which cocks a wheel. The coin then drops into the drop chute, and the signal goes thru a 70 msec delay to allow the coin to clear the mechanism. Then, a unijunction transistor (UJT) circuit pulls in a relay solenoid, which unwinds the wheel until it returns to its start position. The number of times the relay ticks, while pulling the wheel, is the number of beeps. If the wheel went five notches forward, a switch drops, programming the unit to do 35 msec beeps (quarter). However, regardless of the coin used, the first beep will be delayed 70 msec to permit the coin to clear the mechanism.

See the figures for the precise waveforms. These beeps are critical. If not precisely produced, fraud will most likely be suspected! If a taperecorder is used, it must be a high quality one that runs 7.5 IPS or faster.



When you drop in more than one coin, the beep combinations are appended to each other, as far as waveforms go, but the total number of beeps indicate to the operator the total number of nickel-units deposited. For example, if you deposit a quarter, two dimes and a nickel, the quarter waveform will be produced first, then the waveforms for two dimes (four, 80 msec beeps), then one nickel (one, 80 second beep). The operator will count 10 beeps, indicating a total deposit of 50 cents

COUNTERMEASURES

Bell has implemented these countermeasures:

(1) ANALYSIS OF COIN DEPOSIT WAVEFORMS: Most amateur phreakers build oscillators that produce pulses of constant width, and frequency may not be precise enough. Thus, the poor attempt to simulate the quarter will immediately reveal that the payphone is being boxed! However, if the beeps are almost perfectly replicated, this countermeasure is avoided.

(2) COIN SENSE RELAY: Bell operators can inspect the coin sense relay's pull-in current. This relay is activated by the plastic vane which senses the presence of money. The coin sense relay cannot be made to activate anywhere in the system, except by the actual contact of money with this vane. However, Bell can't use the relay to verify money deposited until the operator drops the money into the phone's cache. Since all of the money is dropped the same time, all one needs to do to beat this countermeasure is to actually deposit one coin (or slug) because even a nickel deposit activates the relay the same as \$10 in coins! Further, since the deposit for the first three minutes is automatically dropped and does not go thru the vane-relay mechanism, no seed coin need be deposited to use the first three minutes.

When one makes a LD call from a payphone, the operator comes on to tell him what to deposit for the LD call. She then returns the initial quarter. This resets the coin relay in the open position and removes the relay from the circuit. After one has made his Red Box beeps, the operator need only to check relay continuity to verify if money was actually deposited. If the relay circuit is still open, she will suspect boxing.

(3) DIGITAL OUTPUT: We have been told that Bell is upgrading its payphones to provide a silent digital data output to tell its computers precisely how much money was deposited. This is in addition to the coin beeps. When phones are boxed, only the beeps result. The absence of the digital output will alert Bell to boxing attempts.

(4) ACCOUNTING PROCEDURES: Each call that is made from a payphone requires the deposit of a certain amount of money. These recorded deposits are accounted for at the billing office on a monthly basis, and a computer printout results. The computer amount then is compared to the actual amount collected from the payphone. When a payphone starts going short, Bell immediately checks to see if it is because of an electromechanical failure in the phone, operator error, data processing problem, external theft or internal theft. If Bell concludes that the shortage is due to external theft, or finds slugs or tampering evidence, it then more closely scrutinizes activity at that phone to determine a fraud pattern. Phreakers, like everyone else, tend to develop habits, certain locations may be favorite hang-outs for "phreaker types," and certain payphones get the reputation of being easier to rip-off (the worst gets around). Bell security and the police will then stake out the phone. The clever phreaker always avoids predictable behavior, reputation and "popular" phones.

(5) INCORRECT TONES: Some payphones use a dual tone (1700 Hz and 2200 Hz), but most still use only (2200 Hz). The presence of a dual-tone where not appropriate will trigger suspicions. Since most payphones still use 2200 Hz only, if one doesn't know, it's safer to go with the single tone. One can tell if a payphone is dual or single by having a phreaker call him from it. Have him deposit coins (or slugs). The phreaker will hear the tones and be able to tell.

Continued On P. 7

5 PROGRAMMABLE BLUE BOX

This box has excellent stability with voltage and temperature. It uses 9 common ICs and two 9-volt alkaline batteries. Quiescent current is about 25 ma, use current is about 30 ma. This Blue Box is capable of producing all 15 MF codes. Other codes, such as CCDE 11 and CCDE 12, can be included just by adding input switches and appropriate diodes, and wire up the respective outputs of the analog switches.

When a key is pressed, the diode matrix in Fig. 1 produces a binary code on Lines A-D, corresponding to the key pressed. Note that the code "0000" is not used here, it is reserved for 2600 Hz. Whenever a key is pressed, the S Line also goes high, indicating a valid code on Lines A-D.

In Fig. 2, Lines A-D and S go into the 2519 - a hex 40-bit Shift Register (SR). Only five of the six SRs are used. The input of the 6th. should be grounded. The S Line also goes to a debouncing circuit and schmitt trigger composed of the two inverters and associated parts. The NAND gate takes either the signal from the schmitt trigger or the system clock and generates the clock signal for the SR. This is a neg.-going pulse of about 20 usec. Each time a key is pressed, the data at the input to the SR is shifted in. An LED lights whenever a key is pressed to indicate this.

When all numbers are entered, and one wishes to send tones, the SEND Key is pressed. SEND triggers a Flip-Flop (FF) formed by two NOR gates, and it does four things. It inhibits the input circuitry from the keyboard so no more numbers can be entered; it latches the recirculate line of the SR high so the data is not lost when it is sent, it enables the output circuitry by way of the EO line, and it enables the system clock to shift out the data.

When data is shifted out of the SR, it appears on output Lines A-D. In Fig. 3, these go into two groups of analog switches. Each group contains 16 switches. A binary code at the input of these switches connects the corresponding output to the Z input of the 4051s (ex: if the code "0011" is present at the input, output Line 3 is connected to Z). This places the correct resistor for the desired tone in the circuit. Line O is used for generating the 2600 Hz tone. Each shift of the SR thus places data at the input of the analog switches and selects the proper resistors for the two oscillator circuits. The outputs of the oscillators are summed thru the two 3.3 Kohm resistors and sent to the phone earpiece. The tones are gated ON and OFF by the NOT-EO Line. When all the tones are sent, the S Line goes from high to low and resets the send and clear FFs.

A few additional operational details:

The CLEAR Key triggers its own FF (formed by the other two NOR gates), and does the same things as the SEND Key with two exceptions: The recirculate line of the SR is held low, thus clearing memory and the two oscillators are not enabled so no tones are produced.

The DEL Key is used to delimit between sequences of numbers. When pressed, it clocks the SR without placing any data on its input lines. This fools the circuitry into believing that all the lines have been sent.

The 2600 Hz tone is generated by pressing the SEIZE Key. This is the only key that does not use the common bus. When pressed, it enables the oscillators. And since the only data at the input to the analog switches is "0000" when MF tones are not being sent, the top oscillator generates 2600.

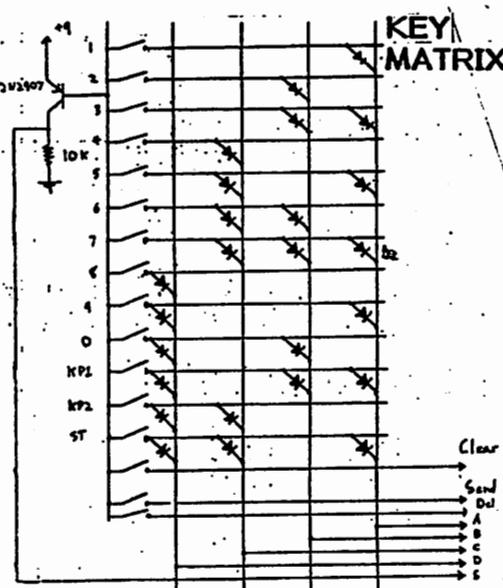
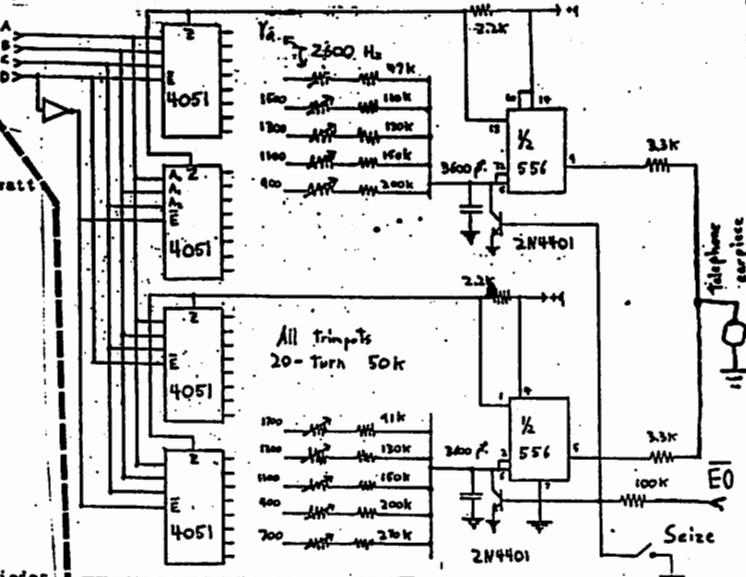
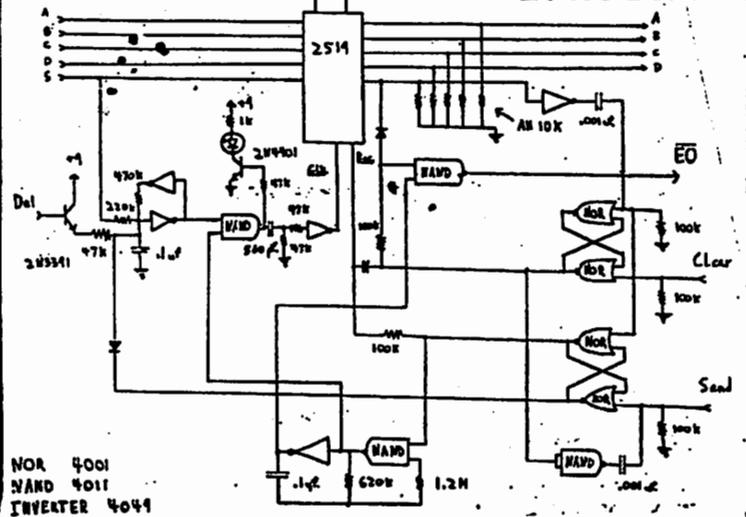
CONSTRUCTION: All ICs, except the SR, use only +9 VDC. The SR also uses -9 VDC. Both the Vss and Vee of the 4051s should be grounded. Vdd is +9 VDC. The input to one unused SR should be grounded. The LED is needed although it does use power - at a glance it can tell if the data has been accepted or when memory is clear.

CALIBRATION AND USE: There are a few methods that can be used to calibrate this box. A DIP switch can be added to the output of the SR to pull these lines up to +9 VDC. If this is used, set the switch to the code for the desired key (ex. "0101" for Key 5). Then press the SEIZE Key to enable the oscillators. One can also wire up a 16-pin plug that can be used to replace the SR. Connect the input pins to their respective outputs and substitute this plug for the SR. When a key is pressed on the keyboard and the SEIZE Key is held, the desired tone is heard.

To use this box, first clear memory by pressing the CLEAR Key. Enter the desired numbers by pressing the respective keys. The LED should light each time a key is pressed to signify acceptance of that entry. Next, call an 800 number and press the SEIZE Key for about one second. When "Ker-chunk" is heard, one counts three seconds, then presses SEND. Out comes the merry tune!

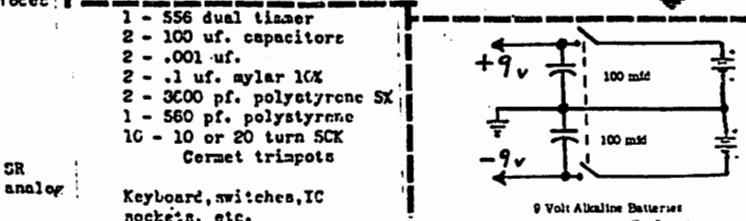
The DEL Key is used when it is necessary to separate sequences of numbers, such as for overseas calls (ex. to call "044 1 246 8000", enter "KP 011 044 ST" then press the DEL Key and re-enter "KP 044 1 246 8000 ST"). When the SEND Key is then pressed, the first sequence will be sent out, then the box will halt. Press the SEND Key again, and the normal sequence will be sent out.

PROGRAMMABLE BLUE BOX LOGIC BOARD



PARTS LIST

- All resistors are 1/2 watt
5% carbon film
- 6 - 10K
 - 10 - 100K
 - 1 - 620K
 - 1 - 1.2K
 - 1 - 220K
 - 1 - 470K
 - 1 - 270K
 - 2 - 200K
 - 2 - 150K
 - 2 - 180K
 - 1 - 11K
 - 1 - 91K
 - 5 - 47K
 - 2 - 2.2K
 - 2 - 3.3K
 - 1 - 1K
 - 1 - Red LED
 - 28 - 1N4148 signal diodes or equiv.
 - 1 - 2N3391 or equiv.
 - 2 - 2N4401 or equiv.
 - 1 - 2N2907 or equiv.
 - 1 - 4001 NOR
 - 1 - 4011 NAND
 - 1 - 4049 INVERTER
 - 1 - 2519 40 bit hex SR
 - 4 - 4051 8 channel analog switch



Keyboard, switches, IC sockets, etc.

9 Volt Alkaline Batteries

6 AUTOMATIC BLUE BOX

The Automatic Blue Box is similar to the Programmable Blue Box, except that more than one phone number can be stored in it. In this version, five 10-digit numbers can be stored. Each number is produced automatically from the touch of a single key. Quiescent current is 40 ma, and it uses a single 9-Volt alkaline battery.

NUMBER ENTRY: Assume that the box has been cleared and a "1" (high) is in all 64 bits of each register. The switch enabling the keyboard is closed. Now press KP; lines for the 1100 Hz and 1700 Hz go low. A "0" (low) is placed on Pin 15 (Data In) of IC-9 and 12, but the data is not entered yet. At the same time, Pin 4 of IC-5A and Pin 13 of IC-40 go low which drives Pin 11 of IC-14C low. This, in turn, makes Pin 10 of all the SRs low thru IC-4A and IC-16B. This puts the SRs in data entry mode. Meanwhile, charge is leaking off C3 thru R14 and, after about 9 msec, QD goes high and NOT-KD' goes low. This delay is to allow for contact bounce in the keyboard switches. QD high drives Pin 2 (Clock Input) of all of the SRs high. The data present at Pin 15 of all of the SRs is now entered. NOT-KD' went low after 9 msec which, thru IC-6A, ICs-17A-F, and ICs-21E-F turns ON the output amplifier (LM386), giving an audible click and lights the pulsing gate indicator LED. The LED stays lit as long as any key is depressed.

The Schmitt triggers (ICs-18E-F) may be 4047s or 74C14s. The 4031 SR, unlike other CMOS ICs, has a large clock input capacitance (Pin 2), so it works better when driven by more than one inverting buffer output.

RUN MODE: Assume that two 10-digit numbers each with a prefix of KP and a suffix of S have been entered into the SRs. I will first describe the 1-of-2 Data Selector (DS) composed of NAND gates, ICs-3B-D, and inverting buffer, IC-16C. Two clock rates are used: 1280 Hz supplied by the oscillator IC-23; and 10 Hz at the output (Pin 3) of the divide-by-128 counter (IC-20). The 1280 Hz clock goes to one input of the DS (Pin 9, IC-3D), while the 10 Hz clock goes to the other input (Pin 12, IC-3C). The control signal appears at Pin 4 of the NOR gate, IC-15B. When the control voltage is low, the output of the DS (Pin 4, IC-3B) follows the high-speed clock. When this pin is high, the output of the DS follows the low-speed clock.

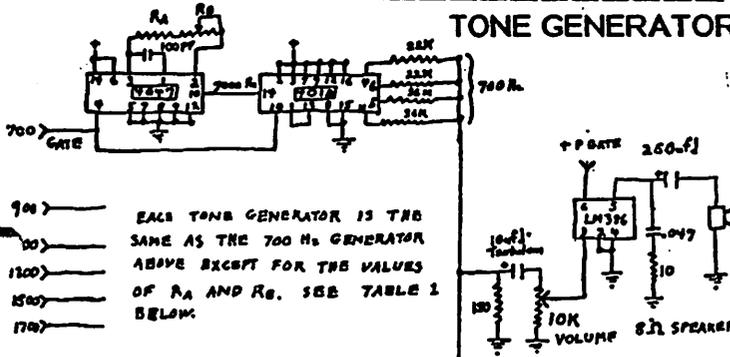
Now, press the RUN Key. IC-4B's Pin 4 immediately goes high and stays high for 50 msec, and the output of the NOR latch composed of ICs-13C-D goes high which sends Pin 3 (IC-14A) low. After

50 msec, this turns the clock ON (IC-23, Pin 4), and drives Pin 1 of IC-6A high which turns ON the output amplifier and the P-gate indicator.

A total of 24 digits have been entered into the SRs. Since these are 64-bit SRs, the data is 40 bits away from appearing at the output. The two NAND gates (IC-5B and IC-4D) see all "1"s at the Q output (Pin 6) of the SRs. This thru IC-15D. IC-15B then selects the high-speed clock, so, at a rate of 1280 Hz, data is stepped thru the SRs.

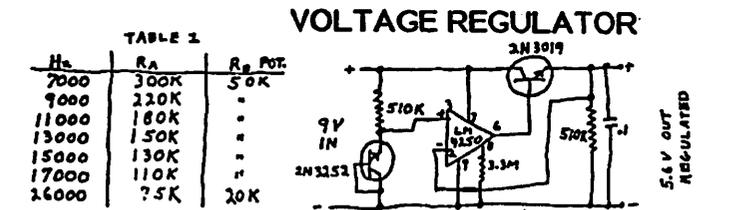
After 40 clock cycles, two things happen, either of which will reset the RUN latch and turn OFF the clock. The "End of Register" (EOR) counter (IC-19) has reached a count of 64 (it also counts when numbers are entered), placing a high level on Pin 6 of IC-14B. Also, the K1+K2 detector composed of the 3 NAND gates (ICs-2C-D and IC-3A) has detected KP1 at NOT-Q output (Pin 7) of the 1100 Hz and 1700 Hz SRs. This places a high level at the other input (Pin 5) and the NOR gate IC-14B. The negative-going pulse at Pin 6 of the reset generator (IC-22) triggers a 2 msec output pulse at Pin 10. This resets the RUN latch, the EOR counter (IC-19), the divide-by-128 counter (IC-2C), and turns OFF the clock. All this happens in 81.25 msec, 50 msec delay before the clock turned ON plus 31.25 msec to shift 40 bits thru at 1280 Hz.

Now, to play the numbers back. The next press of the RUN Key gets the first number. KP of the first number is at the output of the 1100 Hz and 1700 Hz SRs. The output of the K1+K2 detector is high, making trigger input (Pin 6) of the reset generator low but this doesn't do anything. The reset generator is negative-edge-triggered. Let's press RUN again. Again, we get the 50 msec delay before the clock turns ON. The "No Data Detect" gates see data present at the SRs so the DS selects the low-speed clock. Pin 13 of the NOR gate (IC-15C) goes low and Pin 12 of the same IC is also low because it takes 64 clock cycles before Pin 3 of IC-20 will go high. IC-15C then drives one input of all the output NAND gates high (ICs-1A-D and ICs-2A-B). Pin 7 of the SRs IC-9 and IC-12 are also high so the output of NAND gates IC-1C (1100 Hz) and IC-2B (1700 Hz) go low which turns ON the 1100 Hz and 1700 Hz tone generators. The output amplifiers and the "P" gate indicator are also ON so we have 100 msec of KP as per specs. KP is 100 msec because of the 50 msec delay before the clock starts running (the reason for the 50 msec delay). Therefore, R2 and C2 should be chosen to give a 50 msec delay.



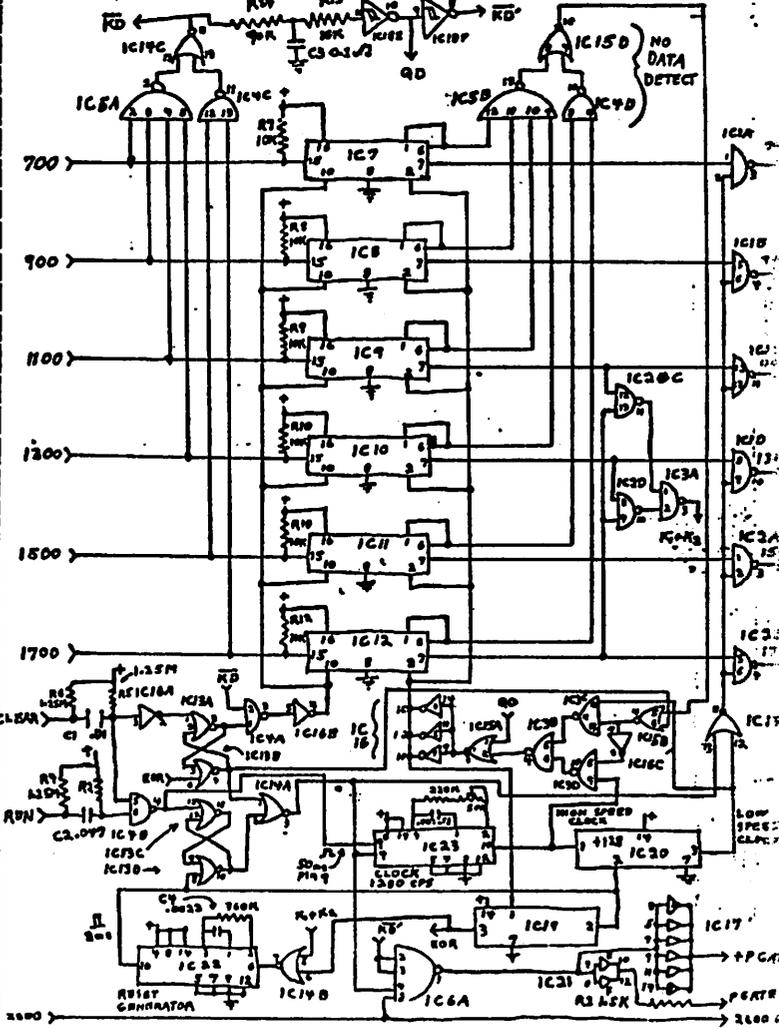
900) — EACH TONE GENERATOR IS THE SAME AS THE 700 Hz GENERATOR ABOVE EXCEPT FOR THE VALUES OF RA AND RB. SEE TABLE 1 BELOW.

Hz	RA	RB POT.
700	300K	50K
900	230K	"
1100	180K	"
1300	150K	"
1500	130K	"
1700	110K	"
1600	75K	20K



- ### PARTS LIST
- IC1, 2, 3, 4, 4011 Quad dual input NAND gate
 - IC5, 6-Dual 4 input NAND gate 4011
 - IC7, 8, 9, 10, 11, 12-4031 64 bit shift register
 - IC13, 14, 15-Quad 2 input NOR gate 4001
 - IC16-Hex inverting buffer 4049
 - IC17-4050 Hex non-inverting buffer
 - IC18-74C14 Hex inverting Schmitt trigger buffer
 - IC19, 20-4024 7 stage binary counter
 - IC21-4050 Hex non-inverting buffer
 - IC22, 23-4047 Low power Monostable/Astable multivibrator

AUTOMATIC BLUE BOX LOGIC BOARD



BLACK BOX

The basic Black Box is shown in (A). When the switch is opened, current and sound can only pass thru the resistor and capacitor. The purpose of the resistor is to provide enough current so that the phone mouthpiece can be powered enough to be heard but not enough to tell Bell that the phone is in use. The purpose of the capacitor is to block DC while permitting the AC voice wave to be transmitted. Although a 0.5 uf capacitor is usually adequate, if one has a bass voice, 1.0 uf works better to allow less attenuation of the lower frequencies. A non-polarized capacitor should be used, rated at least 150 volts. When the switch is closed, the phone acts normally. To perform the ring-stop function, the switch is closed and the phone is quickly picked up and hung up. Then the switch is opened and the conversation can take place without having it interrupted by rings.

The circuit in (B) is from **ABBIE HOFFMAN'S STEAL THIS BOOK**, no longer available anywhere. Except for the use of the 100 uf capacitor and the 10 ohm resistor, (B) is identical to (A). The purpose of such a large capacitor is to act as the "ring-stopper" when one picks up the phone for the first time. This saves the step of picking up the phone fast and quickly hanging up. The 10 ohm resistor is used to safely discharge the capacitor when the switch is switched back to "Free." (B) has three disadvantages over (A):

(1) A non-polarized 200 Volt, 100 uf capacitor is much larger than a 200 Volt, 0.5 uf capacitor.

(2) A 100 uf capacitor is easier to detect by Bell than a 0.5 uf capacitor.

(3) One could make the bad mistake of lifting up the phone in the "Free" position to receive an operator-placed LD call. (B) forces one to do a quick pick-up-and-drop to stop the ringing, and is more conducive to developing the habit of determining which calls to box.

(C) is identical to (A) except that two 52 Volt zeners, wired back-to-back, are also placed in parallel. The phone is picked up after the switch is opened ("Free"), and the ringing voltage avalanches one of the zeners. The surge makes the line voltage sharply drop, which stops the avalanche and the ringing. The two zeners are much smaller than the 100 uf capacitor, the resultant surge is much sharper, and they are more difficult to detect.

(D) uses a PushButton (PB) ring-stopper and a battery to power the mouthpiece. The PB switch provides manual control over the surge required to stop ringing. One starts with a sharp tap. If that doesn't stop the ringing, increasingly longer taps are applied. The purpose of the battery is to provide more power to the mouthpiece to increase conversation volume. Note that the 6 Volt battery is in series with a 240 ohm resistor. This provides 25 ma of voice current. A 9 Volt battery (360 ohm resistor) or a 12 Volt battery (480 ohm) can also be used. Do not use a DC power supply driven by an AC voltage as severe hum can result.

(E) is a Black Box using a 56 Volt zener and a diode in series as the ring-stopper. In the "Normal" position, the ring-stopper and the RC pair are out of the circuit. When the switch is thrown in the "Free" position, the Tip and Ring will momentarily be shorted together to stop the ringing. This circuit requires observing line polarity. In phones correctly hooked up, the Ring is red and positive. Check anyway.

(F) is a variation of (E) to produce greater volume. A 1.0 Kohm pot. is used to vary voice volume. The 10 Kohm current-passing resistor is not required.

(G) is (E) but with an answering service connected. Please note that only answering devices equipped with A and AI terminals can be connected this way. Only the better machines have these terminals marked. If not clearly marked, check out the schematic to determine if and where they are at.

(H) is another Black Box, this one with a built-in LED Snoop Lite.

(I) is a Black Box that is the same as (F) except a full-wave bridge rectifier is used. The purpose of the bridge rectifier is to permit the device to work regardless of Tip and Ring polarities.

(J) is another working Black Box. Little is known about this one.

(K) is a table that describes the Ring-Tip voltages for various phone conditions.

NOTE: Bell phone circuits normally operate from 48 VDC batteries, and use a 105 VAC, 20 Hz ringing current. On-hook voltage should be 48 VDC. Ring voltage should be the 105 VAC superimposed on the 48 VDC. Off-hook voltage should be 6 VDC.

Because there are substantial variations nationally in these voltages, one experiments with the optimum Black Box configuration. Usually, the further one is from the CO, the less these voltages are. By measuring for the 48 VDC, one can estimate line resistance. If the

voltage is nearly 48 VDC, the 10 Kohm resistor should start at 12-15 Kohms. If the line voltage is low, 8-9 Kohms is used.

To check out the Black Box, one lifts the receiver to his ear. A normal dial tone should be heard for the "Normal" switch setting. Switching to "Free" should result in a 1-2 second dial tone followed by the line clearing with the usual soft white noise. If it takes more than 2.5 seconds to clear, it means that the Box resistor is probably 1-2 Kohms too small because Bell's relays are behaving marginally. If the phone doesn't clear at all, the resistor is probably at least 2 Kohms too low.

To static-check a manual ring-stopper, one picks up the receiver as before and clears the line by switching to "Free." He then hits the ring-stopper PB switch. Dial tone should result, and the line should clear again. If not, the circuit is wired wrong.

For a dynamic test, a phriend calls the phreaker from a LOCAL payphone. When the phone rings, he switches the Box to "Free" and taps the manual ring-stopper PB (if the Box has a manual). The phone should stop ringing. He then picks up the phone and answers it and talks to his phriend for a few minutes. He then gets the phriend to hang up first. When the phriend hangs up, the phreaker should hear the return of the phriend's coin and no new dial tone. If the phriend's coin is not returned and a new dial tone comes on, the Box didn't work. If it didn't work, it could mean bad wiring but it usually means that the ring-stopper surge is too long or that Bell has installed some super-sensitive equipment on his line.

Also note that Black Boxes (as well as Blue Boxes) will not work where ESS has been installed because ESS does not permit a direct connection between the origin and destination phone except during the period that the phones are answered and billing is in progress. In ESS, the ring you hear is one that is computer-generated by your local CO.

When you start to ring, 105 VAC (20 Hz) is superimposed across the VDC Tip and Ring lines. In the zener ring-stopper, when the combined voltages exceeds 56 volts, the zener conducts more and more until enough current flows to signal the CO to disconnect the ringing (within a few milliseconds of the first ring pulse). In some cases, the zener voltage may be too low so that when it does avalanche, it will stop the ringing but it won't conduct enough current to signal the CO. This problem is corrected by using a higher voltage zener, perhaps at 70 volts.

To notify the destination equipment that it is about to receive routing information, the originating end first sends a Key Pulse (KP) tone. The digits are then sent. At the end of sending the digits the origination CO sends a Start (ST) tone. Thus, to call 914-359-1517, the CO equipment sends, (KP)+9143591517+(ST) in MF tones. When the customer hangs up, the CO again sends a 2600 Hz tone to signify a disconnect at the destination end.

NOTE: Each dual-tone lasts exactly one second with exactly one second pause between each dual-tone. And both tones in each dual-tone must start and stop simultaneously. MF tones start three seconds after "offing" the line. In modern systems, pulse shape is trapezoidal - not square or sinusoidal.

To use a Blue Box, one usually starts with a call to a Black Boxer phone, service call number, recorded message number, toll-free number, or distant directory assistance (NPA-555-1212, NPA - Area Code). 800 numbers are preferred since Bell started supervising LD directory assistance calls, and Bell flags directory assistance calls over three minutes long. "Supervising" simply means that, when the call is answered, the TO notifies the local office to begin billing. If one "offs" a line that has "returned supervision to him," he will be timed out by his local CO, and he will lose the circuit within 15-30 seconds.

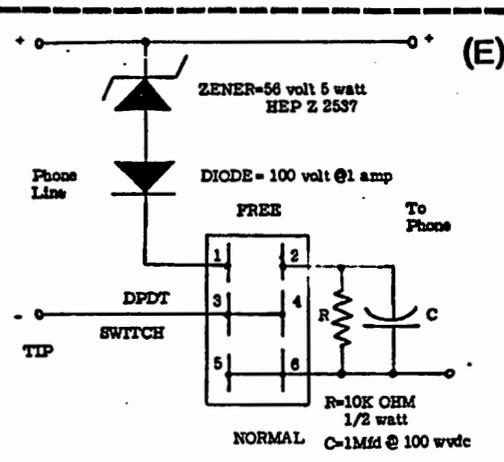
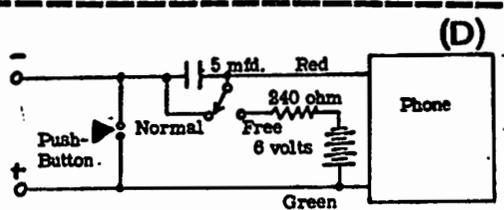
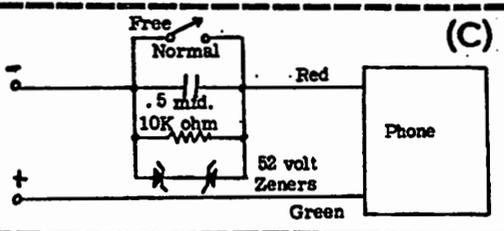
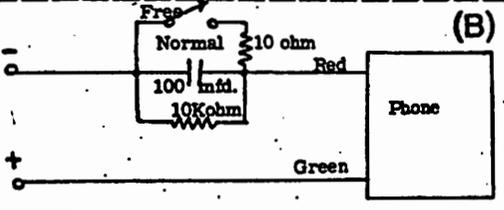
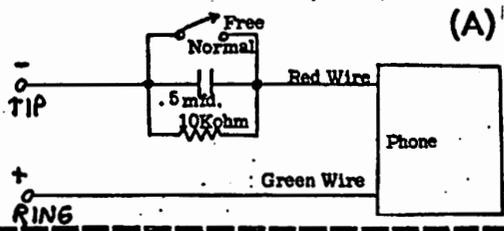
Just when the call is answered, one pushes the 2600 button on his Blue Box. This makes the destination CO equipment behave as if the call had been hung up, thus leaving the trunk to the destination hanging open. Injecting 2600 Hz for this purpose is also known as "offing." The phreaker then has about 10 seconds to enter in the number he wants to dial (in MF tones: (KP)+Number+(ST)). The CO equipment acts as if this call was a normal one from another CO and processes it. Since there are no USUAL billing records of these MF tones (except on toll fraud detection devices!), the user is not billed for the call. When the user hangs up, the CO equipment simply records that he hung up on a free call.

COUNTERMEASURES

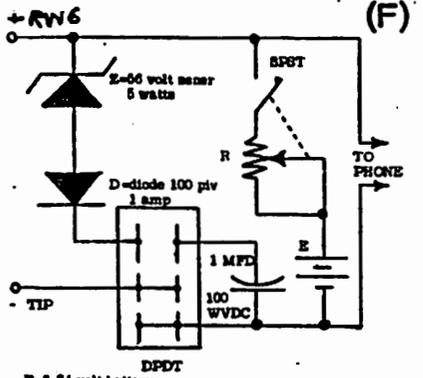
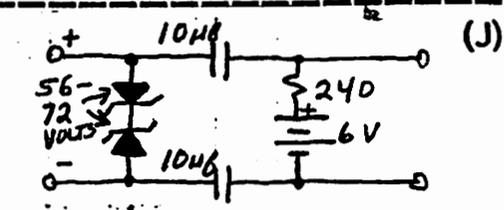
Bell first discovered that Blue Boxes were being used in 1961, and implemented countermeasures in 1964. These countermeasures have steadily increased in sophistication and areas covered since then.

Continued Next Page

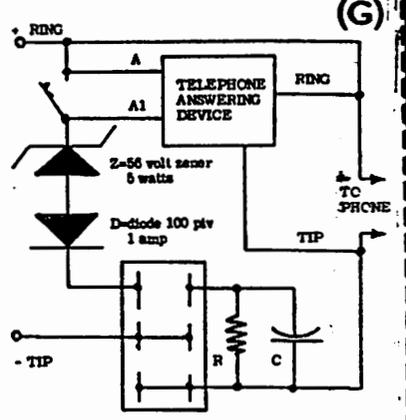
BLACK BOXES



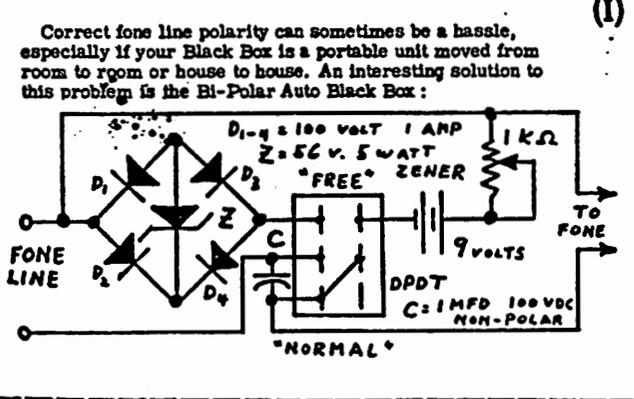
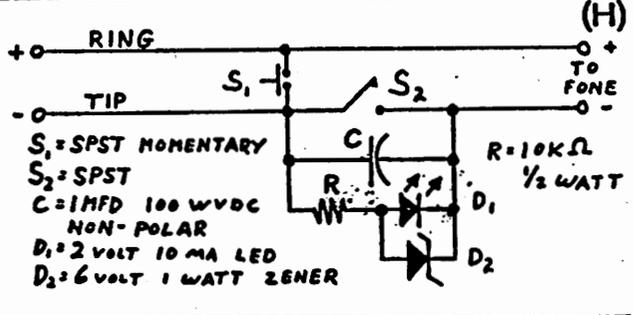
Terminals 3&4 are connected together as are 5&6 but there is no connection between terminals 1&2. With the DPDT switch in the normal position the ringing voltage is across the phone ringer and not across the "answering" diodes. Only when the switch is put in the "free" position are the diodes placed across the line to momentarily "answer" the phone for a few milliseconds. I cannot think of a more appropriate time to build this improved automatic Black Box.



E-6-24 volt battery
R=1 KOhm Pot, audio taper with on-off switch
The standard 10 K ohm resistor is NOT needed. The capacitor passes the audio but blocks the DC voltage which results in an "on-hook" condition. The 1 K ohm pot gives you a level control for YOUR voice.
And speaking of Black Box modifications here's a circuit sent in by a reader from Brooklyn, N. Y. on how to connect a phone answering device to the Auto Black Box:



DPDT
R=10 KOhm resistor, 1/2 watt
C=1 MFD capacitor, 100 wVDC



Correct fone line polarity can sometimes be a hassle, especially if your Black Box is a portable unit moved from room to room or house to house. An interesting solution to this problem is the Bi-Polar Auto Black Box:

	VOLTS	Ma	OHMS	FREQ	TIME
ON-HOOK	48	0	INFINITE	DC	-
OFF-HOOK	8	40	100-200	-	-
RINGING	105	23	-	20	-
BUSY SIG	-	-	-	480+ 820	80 IPM
BLACK BOX RESISTOR	45	4.5	10 Kohm	-	-
DIAL TONE	-	-	-	350+ 440	-

PHONE 9 COLOR BOXES

Consumertronics Co.
2011 CRESCENT DR.
P. O. DRIVE 537
ALAMOGORDO, NM 88310

BLUE BOX TONES

Digit	Freq.s (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
KP	1100+1700
ST	1500+1700
?	700+1700
?	900+1700
?	1300+1700
Disconnect	2600
?	= Unknown Uses

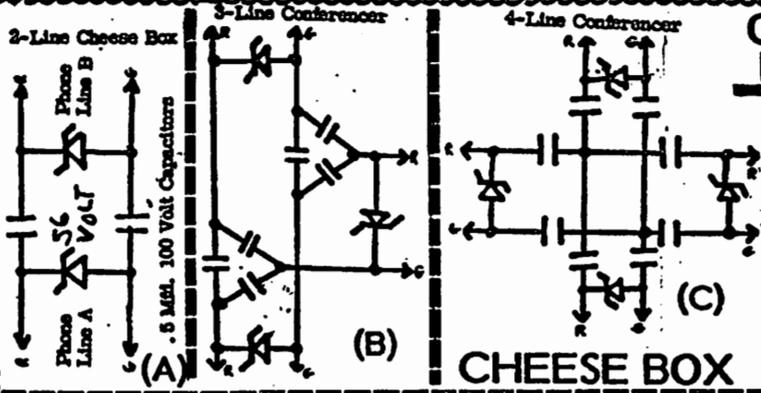
TOUCH-TONE TONES

Digit	Freq.s (HZ)
1	697+1209
2	697+1336
3	697+1477
4	770+1209
5	770+1336
6	770+1477
7	852+1209
8	852+1336
9	852+1477
0	941+1336
*	941+1209
#	941+1477

The uses, if any, of all other possible frequency combinations are not known.

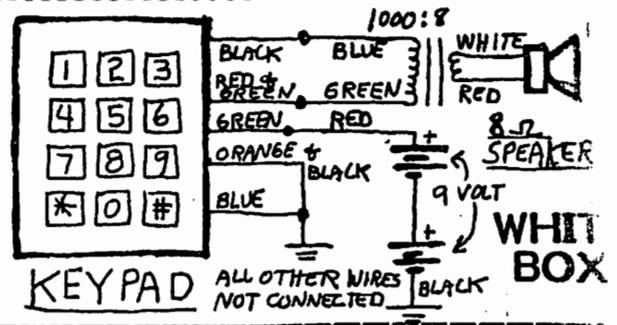
(1) LINE SCANNING: In most large cities and populated states, most (if not virtually all) Blue Box calls are readily detected, as the phone lines are now rapidly scanned by detection devices. The primary thing checked for is the presence of a pure 2600 Hz tone on a subscriber line (where it has no business). Also, if the MF tones don't take on the characteristics described above, more sophisticated equipment will automatically flag the call. If an equipment malfunction doesn't account for the out-of-spec. MF tones, Bell assumes that the call was boxed. On a crossbar system, it drops a card. Under ESS, a printer screeches quietly with the

full details and Bell security is immediately alerted. The basic approach of the scanner is to look for a 2600 Hz tone where one does not belong. Bell then automatically records both numbers, time of day, duration of call, and perhaps the phone conversation itself! In some cases, Bell will then immediately call back and inform the phreaker that he has been caught, that he will be billed fully for the charge, and warned of the penalties for his crime. In other cases (particularly payphones), Bell security and the police rush to the phreaker's location where he is sometimes apprehended in the middle of his boxed call!



CHEESE BOX

OTHER BOXES



The Cheese Box is simply a conference line, or loop around. They are very popular with bookies for bet-placing by phone. Their clients call one number, the bookie calls another, and they are connected together at a third remote location (the Cheese Box). The police won't find the bookie or client at either number. Cheese Boxes not only effectively eliminate call tracing but they are easy to build, and they still work! Care is taken so that phone calls don't exceed three minutes.

Bell-installed loops are limited because they often disconnect after certain time, the numbers must be called in a certain order, and they are often monitored and sometimes even charged. The Cheese Box can be extended to many lines, thereby creating conferencing, will permit either line to be called first, and it will stay on indefinitely. And the Cheese Box is FREE!

Phone voltage is normally about 45 VDC. When the phone rings, an additional ring voltage of about 90 VAC (20 Hz) is received by the called party. In (A), the zener diodes conduct if the voltage rises greater than 56 volts. As discussed under Black Boxes, the zeners act as a ring-stopper. So one can call and his call will be automatically "answered." He then holds on (without being billed or timed) until someone else calls in to the second phone connected to the Cheese Box. The second phone is then similarly answered, and the two phreakers are now connected together and can talk to each other. If the calls are from payphones, upon their completions, the coins will be returned because Bell won't detect that a connection was made.

The capacitors prevent the DC voltages on the lines from interfering with each other. Two are used since a DC connection to either side of the phone can affect each other. The zeners must be properly installed. If not, no dial tone will result.

(B) is a three-phone Cheese Box. (C) is a four-phone Cheese Box. Phreakers normally like to include Cheese Box options with their Black Boxes.

Although the Cheese Box is not a Call Forwarding device, it can be used in that manner. For example, a Cheese Box could be set up using phones registered under fictitious names. The phreaker could call a second party, stating, "As soon as I hang up, call XXX-XXXX." The phreaker hangs up and dials YYY-YYYY, hooked to XXX-XXXX with a Cheese Box. The second party hangs up and calls XXX-XXXX. There might be several reasons for doing this. One reason would be to prevent the second party from tracing the phreaker's origin phone number, which would be impossible in the few seconds it would take him to instruct the second party. Another reason might be that others will engage in the conversation at the Cheese Box location in a three-way conference. The disadvantage of the Cheese Box in a Call Forwarding application over a Call Forwarding device is that the Cheese Box may require a prior instructional phone call.

CLEAR BOX

As explained earlier, the Clear Box is a box used to defeat the type of payphone used in Canada and rural areas. In this type of payphone the call is connected thru first, and you can hear the called party. However, the phone mic. is shorted out until you deposit the correct amount (you can make free calls to weather, 911, and some others).

The Clear Box consists of a 4-transistor amplifier and a telephone suction cup induction pick-up. The induction pick-up is wired to the OUTPUT of the amplifier, and a mic. to its input. The induction pick-up is attached to the rear of the phone. When the called party answers, the phreaker speaks thru the mic., and his voice is inductively coupled to the phone so that he can be heard. This type of payphone does not time out but will stay on indefinitely. The primary disadvantage with the Clear Box is that the volume is usually low and distorted.

The White Box gives you a better understanding of how Touch-Tone phones work, and you will also be able to use tones in payphone that turn OFF their Touch-Tones after you dial your number. In addition, there are phones at airports, hotels and at bank machines which have no dial on them and automatically dial a pre-programmed number (usually a service number). These can be accessed by someone with a White Box to enter a number or numbers before the pre-programmed ones starts to dial, thus gaining control of the phone to dial other numbers - even LD numbers. In some phones after the pre-programmed number is dialed or completed, or an error message ends, the phone reverts to a normal dial tone which makes it accessible to boxing. Before White Boxes, phreakers used to tap out the new number, using the plunger, in the same manner that a rotary dial works (ex: 9 taps = #9).

Portable dialers costs about \$30. Good ones that remember 99 numbers, are password protected, and are smaller than a calculator cost about \$70. Often, they are available from LD services for less when you sign up for them. You can build your own for much less.

Tones made by Touch-Tone phones are not single tones, but dual tones. That is, just as in the Blue Box, two tones are mixed together (Touch-Tones use different tones than Blue Boxes). They are usually referred to as Dual-Tone Multi-Frequency (DTMF) phone. The normal Touch-Tone phone dials 12 dual-tones, but is capable dialing up-to 16 thru internal modification.

The power required by a wired keypad is about 25 volts, but they will operate well at as little as 15 volts, and work fine with two Volt batteries. They are designed to operate with high-impedance phone-type speakers (earpieces) and phone lines, and they do not work with standard 8 Ohm speakers. However, an 8 Ohm speaker required to obtain satisfactory voice volume. To match the keypad to an 8 Ohm speaker, one needs an audio transformer. The smallest 1000-to-8 Ohm audio transformer from Radio Shack is recommended (#273-1380). They are about \$2 each. Buy a handful because they are very handy for all sorts of audio projects - particularly phone circuits - including our TELERECORDER device, see TELEPHONE RECORDER INTERFACE, \$7. You will also need two Volt alkaline batteries and battery clips, a small 8 Ohm speaker, and a small case to assemble these all into.

SILVER BOX

The Silver Box, as stated earlier, is a lineman's handset or REMOBS (Remote Service Observing Systems). They allow Bell employees and phreakers to use the system to tap phones. By using a Silver Box and an ordinary Touch-Tone phone, one can dial directly into the RECEIVE ONLY portion of any customer's line (the mouthpiece is disconnected). Silver Boxes work as follows:

Dial the number of a REMOBS unit. Bell apparently puts them in the 555 information exchange (XXX-555-XXXX). A tone will then be heard for about two seconds and then silence. It is then necessary to key in, with a Touch-Tone, a 2-5 digit security code, holding each digit down at least one second. If the code is not entered within 5-6 seconds, the REMOBS will disconnect, and must be dialed again. If the code is properly entered then another tone will be heard. Any 7-digit customer number can then be entered (the REMOBS can only handle certain exchanges which are prewired for it, and usually one machine can't monitor all of a multi-city locality).

The REMOBS will then connect up to the customer line. The phreaker will hear the low level idle tone. As the monitored party dials, the phreaker will hear the number being dialed and the entire conversation! At no time will the monitored party be aware that he has been tapped - there are no messages, clicks, strange sounds etc.! When the phreaker is done listening to Customer A, he can key in a single "reset digit" (usually the last digit in the access code), which disconnects him from the monitored line and returns him to the tone so that he can dial Customer B. When the phreaker wants to quit, he keys in a single "disconnect digit," which disconnects him from the last line being monitored, and disconnects him from REMOBS so that REMOBS can be reset and be ready for another caller.

One method that foils Blue Box scanner detection is to add some "pink" noise to the 2600 Hz tone. The relevant pink noise consists of frequencies above 3000 Hz; usually 3150-3500 Hz are used. The pink noise makes it up to the local CO, where the Blue Box detection is taking place, but is filtered out by the time it reaches the destination end as LD lines are actually 300-3000 Hz bandpass filters.

Since the CO fraud detection devices look for pure 2600 Hz only, the pink noise will prevent detection of the boxing effort. The TO also looks for pure 2600 Hz. The reason why both offices look for a pure 2600 Hz tone for fraud detection and switching is that if they allowed tone mixtures, music from a stereo could accidentally terminate one's LD call - not to mention trigger a raid on his home!

The Blue Box is modified to add a 3000+ Hz frequency, which is mixed in with the 2600 Hz tone in any proportion, using a trimpot. The trick is to create the optimum mixture of 2600 Hz and 3000+ Hz so that only the CO is affected. The mixture starts with a maximum of 3000+ Hz component so that the line is not "offed." Then the relative proportion of 2600 Hz is increased until the familiar "ker-chink" sound is heard followed by the soft noise that comes from an open LD line. At that proportion, carefree Blue Boxing may be possible.

(2) **ACCIDENTAL:** Keep in mind, that Bell sometimes discovers boxed calls purely by accident. Bell personnel have the LEGAL right to eavesdrop on private conversations, purportedly to "test the quality of the line." So, the next time you tell your girlfriend on the phone how you would like to prove your love for her and you hear a strange giggle, you will know at least what the hand of one Bell employee is doing at that moment!

(3) **LONG CALLS:** If the phreaker uses a payphone, and his call is no longer than a few minutes, he usually gets away with it. And there are even rumors of certain special test numbers that hook into trunks thus avoiding the need for 2600 Hz and the risks of detection.

Probably the most effective way that phreakers defeat the penalties associated with this serious crime is to operate in pairs from payphones. Phreaker #1 boxes his call, then immediately hands over his Blue Box to Phreaker #2, who promptly disappears into the crowd. If Phreaker #1 is then caught, he simply states, "What's going on? Some guy I don't know just now asked me to hold this phone for him." Since no box will be found on Phreaker #1, it will be impossible to prove that he boxed the call. Phreakers have been known to use this technique to test the limits of Bell security.

(4) **OUT-OF-BAND SIGNALING:** Besides the in-band detection schemes, Bell has also begun to gradually redesign the network using out-of-band signalling. This is known as Common Channel Inter-office Signaling (CCIS). Since this signaling method sends all of the signaling information over separate data lines, Blue Boxing is impossible under it. CCIS is still not totally implemented, and, until it is, some Blue Boxing will take place. Still not converted is Canada, WATS numbers and rural areas.

(5) **ACCOUNTING METHODS:** Another method that Bell uses to detect Blue Box fraud is that, by its very nature, it means that the phreaker must get the TO to switch him from an "unsupervised" (free) line to a "supervised" line. Upon offing an unsupervised line to dial a supervised one, a record will be generated of the call. Therefore, a supervisory record generated by an unsupervised call can be easily flagged as Blue Box fraud! Only the dumbest phreakers Blue Box from their homes.

BLACK BOX

The objective of the Black Box is to obtain free LD phone calls, but it works differently than the Blue Box. When you call someone LD, you are billed from the moment they answer. The CO knows that you answered an incoming call by a certain amount of DC current that flows thru the phone. The objective of the Black Box is to eliminate the off-hook current to stop the billing but still permit enough current to allow talking.

Black Boxes are the simplest to build. The simplest ones consist of a toggle switch, resistor and capacitor wired in parallel with each other in place of a section of the green or red line. The toggle switch has two positions, "Normal" and "Free." The "Normal" position shunts the RC network. Normally, the switch is in the "Normal" position. When a phriend calls, the phreaker, who has the Black Box, switches to the "Free" position and picks up the phone. Switching to the "Free" position must be done either before or within 1/2 second of off-hook condition. If later than 1/2 second, billing will have started and the call will be terminated automatically. After finishing the phone call, both parties hang up, and the switch is toggled back to "Normal."

Some operational quirks and problems:

(1) The call must NOT have been placed thru an operator. If so, one is at risk of discovery. This leads to a dilemma because, unless one is absolutely assured ahead of time that a phriend is calling direct, he wouldn't know prior to activating the Black Box whether or not the call was placed by an operator.

The most popular method is for the phriend to call LD, using the operator, Person-to-Person, and ask for a special name. The call is refused and hung-up, and the name alerts the phreaker to expect an immediate LD direct call from his phriend. In fact, this technique is widely used by many folks to signal a called party. For example, when a travelling salesman arrives at a destination, he calls home Person-to-Person. If he asks for one name, it means all is fine. Another means car trouble. Still another means illness.

In fact, the person asked for can be a cipher for a sentence-long message, phone number, etc. I've heard of one case that, whenever salesman "Bob" goes on a trip, he calls his wife "Sue" back collect, Person-to-Person. Not only is this call free, but from the voice he call tell whether Sue is home. He then asks for a fictitious name that, when decoded, reveals the exact phone number that Sue needs to call him back direct on at a much cheaper rate. For example, the name, "Dr. David L. Tyler, II," decodes to the area code, CO number and the last four digits of the phone number where Bob is at. The "Dr." means that the CO number is the fourth highest CO number in that area code ("Mr." is highest, "Mrs." is second, "Miss" is third). The "D" in "David, the "L" in "L." and the "T" in "Tyler" are the first three digits of the phone number. The total length of the name (11) minus 5 is the last digit (6). The "II" means the second area code in his list. Since Bob and Sue have identical lists of area codes and their CO numbers, Sue can determine the area code and the CO number from the "II" and the "Dr.," and the last four digits from the name itself!

Another method used to assure a phriendly call is to have the calling party sing or whistle into the line while it is ringing. The called party then picks up the phone on "Normal" and hangs it up within 1/2 sec. - while listening for this signaling. Ringing may stop. Or he may use a phone tap to listen in on the unanswered line. Knowing that it is a phriendly call, he then toggles to "Fr" and quickly lifts up the phone again.

Another method is to install an infinity-bug-like device that will automatically alert the called party of the phriendly call (thru an external LED or buzzer) to box the call. In the March and April 1984 issues of RADIO ELECTRONICS (two-parts series) are the plans to a device that, among important legal uses, can be applied as such a device. The RE device can also permanently put an end to unwanted phone calls - regardless of the source! The way the RE device works is that when a permitted party calls you, he uses a tone generator or whistle to signal the RE device. Your phone then starts to ring as usual. However, if he does not produce this tone within 10 seconds, your phone never rings and he is automatically hung up on. You also have the option of switching this device ON or OFF as you please.

(2) The Black Box only works where crossbar switching is still being used. It does not work where ESS is used, because, under ESS, there is no direct hookup between the caller and the called party except during billing. Although ESS is being implemented nationally, it will be beyond the year 2000 before completed. You can tell if you have ESS by picking up your phone. If dial tone is immediate, ESS is installed - Black (and Blue) Boxes are useless. If dial tone takes about 1/2 second to come on, they should still work.

(3) The "Free" position tends to terminate all local calls. Thus, local callers might have to phone again.

(4) Calls longer than 15 minutes are especially risky. Bell especially screens long-duration calls for legitimacy.

(5) If one has extension phones, all of them must have Black Boxes connected to them. And they all must be simultaneously switched into the "Free" mode for "Free" use. If even one is placed in the "Normal" mode during a boxed call, billing will automatically begin.

(6) One advantage with the Black Box is that it allows one to monitor his phone lines while not alerting folks who may be using it unknown to you - such as tappers, phone company personnel, etc.

COUNTERMEASURES

As we stated, the implementation of ESS, line scanning for inappropriate low resistances and AC voltages, and analyzing calls based upon their longevity are methods that Bell uses to detect Black Box calls. In the scanning method, OFF lines are scanned to detect any unexpected activity. In fact, Blue and Black Box scanning are usually combined functions. When a Black Box is suspected, the security procedures used are about the same as those used for Blue Boxes with the addition that the detector may force the off-hook condition to automatically start billing.

Also, one result of Black Boxing can be the appearance at the CO of a phone continually ringing. Ringing that persists for more than a few minutes is also investigated as a Black Box call. Most Black Boxes built today have ring-stoppers so checking for long rings is easily defeated.

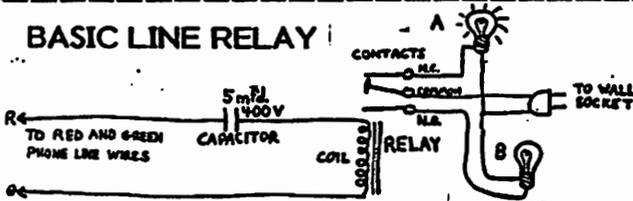
MISCELLANEOUS CIRCUITS

Described below are a number of miscellaneous phone circuits. For many more, refer to **TELEPHONE ACCESSORIES YOU CAN BUILD**, 1976, and **MORE TELEPHONE ACCESSORIES YOU CAN BUILD**, 1980; both by Jules Gilder, Hayden. You can also refer to many phone projects described in **RADIO ELECTRONICS** and the now defunct **POPULAR ELECTRONICS** over the years. We also strongly recommend our **TELEPHONE RECORDER INTERFACE (\$7)**.

SECRET EXTENSIONS

Bell tests for how many extensions you have on your line by measuring the capacitance of the line thru each phone's ring circuitry. You may not care for Bell to invade your privacy this way. The solution is to wire two back-to-back zeners or a transient suppressor in series with the ring circuits in all of your extensions. Avalanche voltage should be at least 52 volts. Choose devices with low capacitances - no greater than 50 pf. Your extensions will then appear as open-circuits to Bell, but will still respond to the 90+ VAC ring voltage.

BASIC LINE RELAY



BASIC LINE RELAY

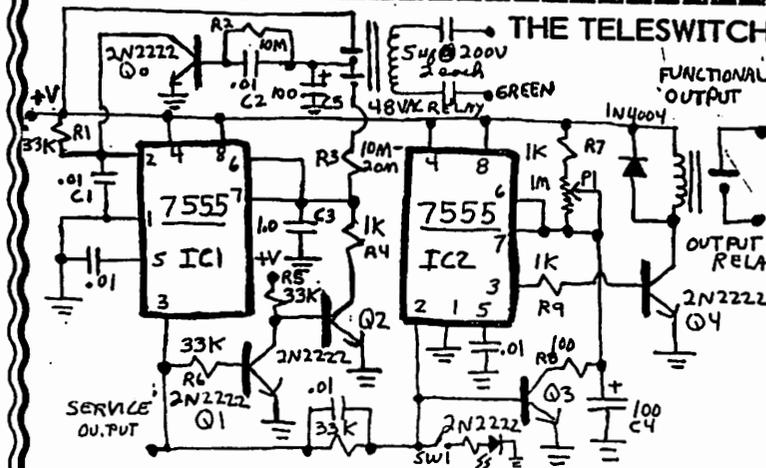
The Basic Line Relay allows you to remotely perform and control functions. Let's say that you're called out of town to do a demo for your bra company, and there's nobody to feed your goldfish! You call your home, and by doing so you activate this device. It then dispenses food so your fish don't starve. The relay activates only during ring, so the number of relay closures or total duration of closures is depended upon the number of rings of the phone.

THE TELESWITCH

Granted, the Basic Line Relay may be overly simple. Your fish might get too much food if others call and activate the relay. The best way to prevent this is to add to this circuit a timer, a tone detector, or number-of-rings detector (counter) so that only you will know how to activate the line relay.

The **TELESWITCH** uses the timer approach. The 7555 timer ICs shown are low-powered CMOS versions of the common 555 timer. Two 555 timers or (one 556 timer) can be used in its place. Prior to ringing, output pins of both IC1 and IC2 (Pin 3) are low. Q1, Q4 and Output Relay are OFF. C1 is charged up to +V, which can be 9-18 VDC. R3 is selected for the desired ring time before activation begins. P1 is adjusted to the required ON time (IC2) of the function desired.

FUNCTIONAL USE: The objective of this circuit is to not activate IC2 until the phone rings for a certain period of time, perhaps after 10 or 20 rings. When the phone starts to ring, the first ringing pulse pulses Q0 thru C2, which shorts C1 to ground. The dumping of C1 triggers IC1 ON thru Pin 2. Output Pin 3 then goes high. When Pin 2 goes high, it turns ON Q1, which turns OFF Q2, thus removing the short across timing capacitor C3. C3 then charges up thru repeated closures of the 48 VAC Relay thru R3 until the threshold voltage is reached (1.1xR3xC3).



KNOWLEDGE + PRACTICE = SURVIVAL!

Consumertronics Co. 2011 CRESCENT DR., P. O. DRAWER 537, ALAMOGORDO, NM 88310

SOLD FOR EDUCATIONAL PURPOSES ONLY

PHONE COLOR BOXES

12

COMMENTS: The **TELESWITCH** is not foolproof. A persistent caller can activate the circuit function. That, in itself might be useful. If someone is using the phone to harass you, it's likely that he will ring persistently. The output relay could automatically activate a recorder to record all persistent callers. This could be used in conjunction with a hook-up to record while the phone is still ringing. This could reveal comments the harasser makes to himself or others between rings - comments he would believe to be unheard.

TESTING: You can get your phone to ring by picking the receiver up and dialing your number. Hang-up just as ringing begins. Your phone should then start ringing. You can also build a ring simulator by rectifying and filtering 120 VAC, then switching it at 20 Hz using a high-voltage transistor. A 556 dual-timer IC can be easily wired so that its first section produces a square wave (2 seconds ON, 3 seconds OFF), and this square wave gates the 20 Hz oscillation of its second section. By doing this, you can fine-tune the **TELESWITCH** to ignore all call attempts up to a certain number of rings.

C5 tops off its charge during rings. The high output of Pin 3 of IC1 turns Q3 ON which shorts C4 to ground thru R8 to remove almost all residual charge on C4. When the threshold voltage is reached, IC1 times out - Pin 3 drops to zero, which triggers IC2 at Pin 2 to begin timing. A zero at Pin 3 of IC1 also turns Q3 OFF, which allows C4 to charge up. When IC2 is triggered ON, its Pin 3 goes high, turning on Q4 and thus the Output Relay. The required function is performed thru the contacts of the Output Relay. C4 charges up thru R7 and P1, and when it reaches its threshold voltage, Pin 3 of IC2 goes low, Q4 shuts OFF and so does the Output Relay.

If the phone is not ringing after function completion, C2 and C5 slowly discharge thru R2. After about 10 seconds from the last ring cycle, these charges will be low enough that the ringing from a new phone call will again trigger IC1 ON. If the phone continues to ring after function completion, the charge of C5 prevents Q0 from being pulsed ON again, thus Pin 2 of IC1 can't be retriggered ON until the ringing stops for about 10 seconds. This prevents unwanted multiple activations due to a continuous ringing.

EXTRANEIOUS CALLS: On the other hand, you don't want other calls to your home or business to trigger the function. Since almost everyone hangs up by five or six ring cycles, the circuit must time beyond that amount. When calls consisting of the usual few rings occur, IC1 is triggered ON as before and its Pin 3 goes high. Unless enough rings occur to charge C3 to the threshold point, IC1 won't time out. Recall that IC2 is activated only after IC1 times out. After the ringing stops, C3 and C5 will start discharging until C3 reaches nearly zero volts. Successive calls that come more than about five seconds apart will not have a cumulative timing effect.

With Pin 3 (IC1) now stuck high, more battery current will be drawn. This might be useful to indicate that at least one person called you after your last circuit activation. However, you can unstick Pin 3 by installing another 7555 (to be called IC3) (or other timer) to time concurrently with IC1 that will reset IC1 thru its Pin 4. The collector of Q1 would be wired to Pin 2 of IC3 to trigger it. On the other hand, a high at Pin 3 of IC1 can be used to activate an answering machine or tape recorder.

As with other boxes, smart Black Boxers don't push their luck by making LD calls over 15 minutes. The shorter, the safer.

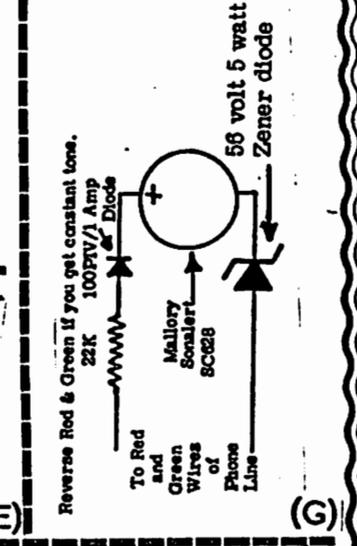
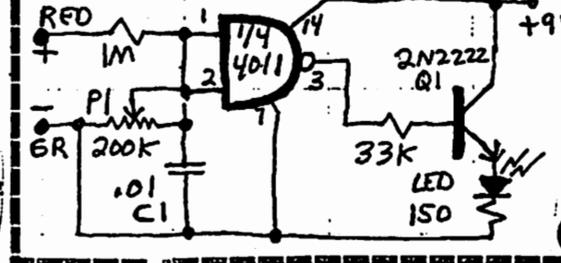
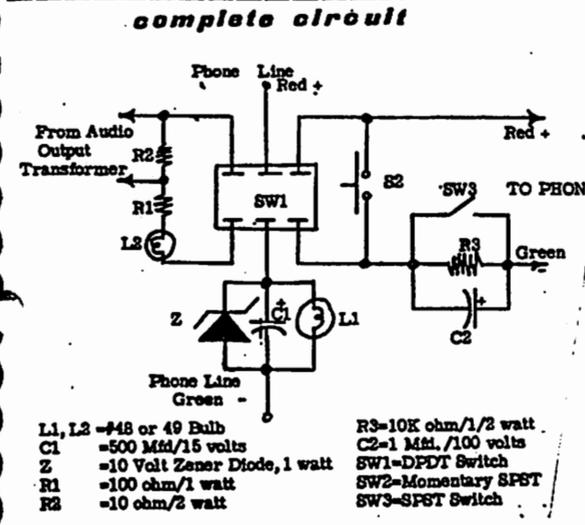
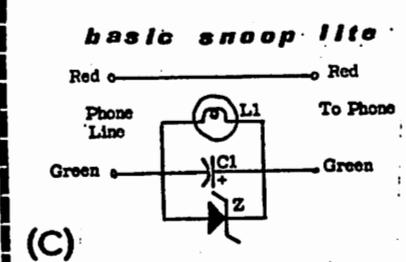
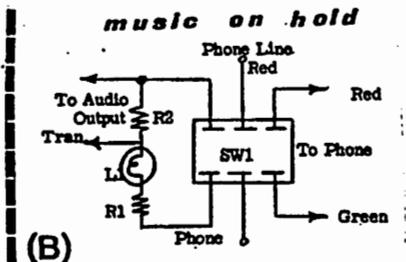
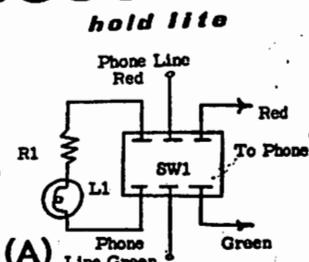
CF BOX

A Call-Forwarding or "CF" Box is one that permits one to make LD call thru a LOCAL phone that has a CF Box installed. The local phone is called and it answers automatically, without ringing. The LD number is then dialed by an automatic dialer hooked up to the CF Box and a second phone line. When the LD call is answered the two phone lines are connected together. The old-style way of doing this was to use two payphones to call two parties, then take or rubber-band the handsets together in the "69" position so that the two parties could talk to each other while neither being able to trace the other.

CF Boxes have these advantages:

- (A) Call origin is almost impossible to trace.
- (B) The intermediate phone - not the call originator - is billed for the LD call. No need for risky Blue or Black Boxes - the LD call is placed like any legal LD call!

Continued On P. 1



OTHER CIRCUITS

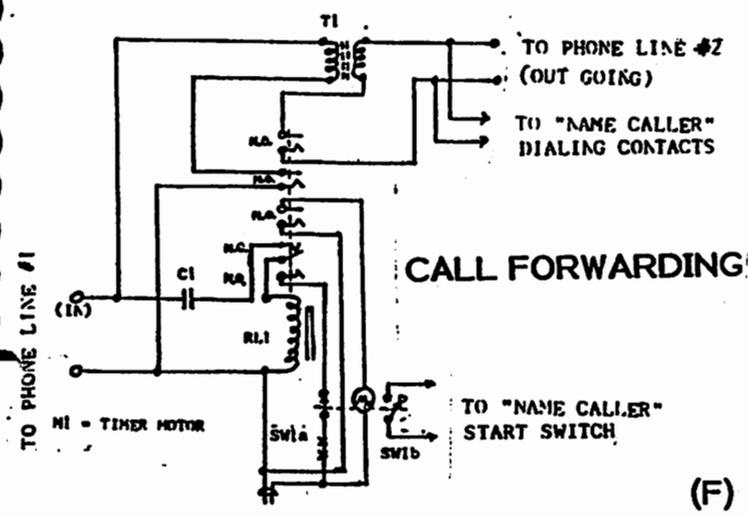
(A): The Hold Circuit allows you to put a call on hold by switching SW1 to the hold position. The Hold Lite then blinks with ring current.

(B): Music-On-Hold is adapting the Hold Circuit to play music into the line.

(C): The Basic Snoop Lite consists of a bulb, capacitor and zener in parallel with each other; all in series with the phone line. The zener prevents disconnection should the bulb burn out. The capacitor shorts out ring current. The bulb draws no current when the phone is on-hook. When the phone is lifted up, the DC current thru the 100 ohms of phone circuit also goes thru the bulb, and the bulb lights brightly.

(D) COMBINED CIRCUIT: Music-On-Hold is combined with the Basic Snoop Lite.

(E): A better Snoop Lite. P1 is adjusted to about 7.0 volts On-Hook, which drops to about 1.1 volts Off-Hook. The output of the 4011 is low during On-Hook and high during Off-Hook. Q1 conducts when its input is high, during Off-Hook. P1 can be adjusted to just barely turn OFF the LED during On-Hook to detect Black Boxes and SOME sophisticated bugs. For greater sensitivity, C1 should be reduced to .0001 uf or less. LED activation will indicate a boxed or bugged call, or fluctuating line voltage. NOTE: This device will NOT detect all modern bugs.



(F) CALL FORWARDING DEVICE: This nifty device allows you to place a local or LD call thru an intermediate phone. Call forwarding devices have legal and illegal applications. They are used, for example, by businessmen so that after-hour calls will be automatically transferred to their home. And they can be used by phreakers to place LD calls. When one calls in, the ring voltage activates RL1, and RL1 switches its activation to the 110 VAC line. Its "B" contacts activate a timing motor or electronic timer. Its "C" contacts activate a timing motor or electronic timer. Its "D" contacts activate a timing motor or electronic timer. Its "E" contacts activate a timing motor or electronic timer. Its "F" contacts activate a timing motor or electronic timer. Its "G" contacts activate a timing motor or electronic timer. Its "H" contacts activate a timing motor or electronic timer. Its "I" contacts activate a timing motor or electronic timer. Its "J" contacts activate a timing motor or electronic timer. Its "K" contacts activate a timing motor or electronic timer. Its "L" contacts activate a timing motor or electronic timer. Its "M" contacts activate a timing motor or electronic timer. Its "N" contacts activate a timing motor or electronic timer. Its "O" contacts activate a timing motor or electronic timer. Its "P" contacts activate a timing motor or electronic timer. Its "Q" contacts activate a timing motor or electronic timer. Its "R" contacts activate a timing motor or electronic timer. Its "S" contacts activate a timing motor or electronic timer. Its "T" contacts activate a timing motor or electronic timer. Its "U" contacts activate a timing motor or electronic timer. Its "V" contacts activate a timing motor or electronic timer. Its "W" contacts activate a timing motor or electronic timer. Its "X" contacts activate a timing motor or electronic timer. Its "Y" contacts activate a timing motor or electronic timer. Its "Z" contacts activate a timing motor or electronic timer.

This version of a Call Forwarding device is not totally satisfactory because it requires two phone lines, and preprogramming of the auto-dialer. Newer circuits we have heard of (but not seen) require only one phone, and, when they are automatically answered, the destination phone number can be sent using a Touch-Tone pad. The caller then hangs on, the CF boxed phone dials the destination phone, then connects the two in a time-multiplexing scheme when that phone is answered. We were unable to acquire any schematics. If you have one, please send it to us with functional description immediately for future editions. We want to devote far more space to CF Boxes, so please send us whatever information you have on them.

(G) REMOTE RINGER: The Remote Ringer uses a Sonalet for the ringing. Similarly to Secret Extension, the Remote Ringer is practically undetectable by Bell. Great for outdoors, garages, sheds, etc., accessible to phone lines.

- MATERIALS:**
- C1= 1.0Mfd @ 400 VDC
 - RL1= 4P.DT Relay, 115 vac coil
 - T1= Audio isolation transformer, approx 600 ohms imped, 100 to 200 ohms DC Res.
 - M1= Timer Motor, 115 VAC 60 CPS
 - SW1a= First section of timer switch, set for approx 3 min closed, 10 sec. open (due to circuit configuration, timer will self-index to "open" position of this switch).
 - SW1b= Second section of timer switch, set for minimum possible duration "on". Indexed to close after SW1a has come out of detent. This is the critical factor in choosing the type of timer. "on" duration must be less than time required for "name caller" to finish dialing.
- ADDITIONAL ITEM REQUIRED, BUT NOT SHOWN:**
- 1, ea. battery powered "Name Caller" dialing machine or equiv.
- NOTE:** Over-ride disconnect switch (Tone Sens. Relay?) may be connected at point X-X.

PARTS LIST

PHONE COLOR BOXES 14

ATARI

```

1 POKE 82,0:POKE 755,0
2 OPEN #1,4,0,"K;"
50 PRINT "ATARI BLUE BOX PROGRAM"
51 PRINT "0-9 = MF 0-9"
52 PRINT "K=KEYPULSE"
53 PRINT "S = START"
54 PRINT "SPACE BAR = 2600 HZ ON/OFF"
55 PRINT "You must press the space bar twice"
56 PRINT "for the program to work correctly."
60 REM
140 DIM N$(1)
144 GET #1,N
145 N$=""
146 LET N$=CHR$(N):? N$," ";
150 IF N$="" THEN ? "2600Hz ";:GOSUB 290
160 FOR LOOP=1 TO LEN(N$)
170 IF LEN(N$)=0 THEN GOTO 500
190 CHAR=ASC(N$(LOOP,LOOP))-ASC("0");TRAP 200;
RESTORE 360+CHAR*10;GOTO 220
200 IF N$(LOOP,LOOP)="K" THEN RESTORE 460;
GOTO 220
210 IF N$(LOOP,LOOP)="S" THEN RESTORE 470;
GOTO 220
215 CLR: GOTO 60
220 READ A,B,C,D
230 POKE 53760,A:POKE 53762,B:POKE 53764,C;
POKE 53766,D
240 POKE 53767,168:POKE 53763,168
250 FOR A=1 TO 15:NEXT A
260 POKE 53767,160:POKE 53763,160
270 NEXT LOOP
280 CLR: GOTO 60
290 SOUND 0,0,0,0:POKE 53768,120
300 POKE 53760,B1:POKE 53762,1:POKE 53764,0;
POKE 53766,0
310 POKE 53767,168:POKE 53763,168
320 GET #1,N:IF N<>32 THEN 320
330 POKE 53767,160:POKE 53763,160
340 N$=""
350 RETURN
360 DATA 165,2,80,2
370 DATA 240,4,210,3
380 DATA 240,4,40,3
390 DATA 210,3,40,3
400 DATA 240,4,165,2
410 DATA 210,3,165,2
420 DATA 40,3,165,2
430 DATA 240,4,80,2
440 DATA 210,3,80,2
450 DATA 40,3,80,2
460 DATA 40,3,8,2
470 DATA 80,2,8,2
480 FOR A=1 TO 700:NEXT A
490 NEXT LOOP
500 CLR:GOTO 60
510 REM --- BY: DEVIUS XEVIUS ---

```

COMPUTER PHONE BOXES

There are two basic types of phreaking using a computer. By far, the largest is Computer Phreaking - that is, using one's computer to invade other private and commercial computers for mischief, mayhem and madness. See our COMPUTER PHREAKING (\$15). Computers are also used for Phone Phreaking.

The newest approaches to phone phreaking is using one's home computer as a sophisticated and programmable box. Some phreakers are also building hand-held Brown Boxes using microcomputer chips.

COMMODORE 64

```

5 B=54272
6 DIM B(7),A(7)
10 FOR LS=S TO S+24:POKE LS,0:NEXT
20 POKE S+5,64:POKE S+6,100
25 POKE S+12,64:POKE S+13,100
30 POKE S+24,15
40 FOR T=1 TO 7
50 READ A(T),B(T)
60 NEXT T
70 PRINT "USE 1-0 FOR DIGITS 1-0"
80 PRINT "USE K FOR KP : USE S FOR ST"
88 PRINT "USE + FOR 11 : USE - FOR 12"
90 PRINT "USE L FOR KP2"
95 PRINT "PRESS SPACE BAR FOR 2600 HZ"
100 PRINT "PRESS THE APPROPRIATE KEY AND
THE TONE WILL BE EMITTED FROM THE TV"
110 GET A$: IF A$="" THEN 110
120 IF A$="S" THEN T=5:U=6
125 IF A$="L" THEN T=4:U=6
130 IF A$="K" THEN T=3:U=6
140 IF A$="+" THEN T=2:U=6
150 IF A$="-" THEN T=1:U=6
152 IF A$="1" THEN T=1:U=2
154 IF A$="2" THEN T=1:U=3
156 IF A$="3" THEN T=2:U=3
158 IF A$="4" THEN T=1:U=4
160 IF A$="5" THEN T=2:U=4
162 IF A$="6" THEN T=3:U=4
163 IF A$="7" THEN T=1:U=5
164 IF A$="8" THEN T=2:U=5
166 IF A$="9" THEN T=3:U=5
168 IF A$="0" THEN T=4:U=5
169 IF A$=" " THEN T=7:U=7
170 POKE S+1,A(T):POKE S,B(T)
175 POKE S+8,A(U):POKE S+7,B(U)
180 POKE S+4,17:POKE S+11,17
190 GET Z$:IF Z$="" THEN 190
200 POKE S+4,16:POKE S+11,16
210 GOTO 110
500 DATA 44,0,57,0,70,0,83,0,96,0,108,
0,166,0
510 REM THE ABOVE DATA STATEMENT MAY
HAVE TO BE ADJUSTED TO GET
THE EXACT TONE.

```

TI 99/4A

FROM BASIC:

```

0: CALL SOUND(100,1300,0,1500,0)
1: CALL SOUND(100,700,0,900,0)
2: CALL SOUND(100,700,0,1100,0)
3: CALL SOUND(100,900,0,1100,0)
4: CALL SOUND(100,700,0,1300,0)
5: CALL SOUND(100,900,0,1300,0)
6: CALL SOUND(100,1100,0,1300,0)
7: CALL SOUND(100,700,0,1500,0)
8: CALL SOUND(100,900,0,1500,0)
9: CALL SOUND(100,1100,0,1500,0)
KP: CALL SOUND(100,1100,0,1700,0)
KP2: CALL SOUND(100,1300,0,1700,0)
11: CALL SOUND(100,700,0,1700,0)
12: CALL SOUND(100,900,0,1700,0)
ST: CALL SOUND(100,1500,0,1700,0)

```

These Brown Boxes will consist of a Blue Box, a Red Box and a White Box at the minimum, and will perhaps double as calculators. To date, we have not been able to find a home-built microprocessor-based box design. If you know of any, please send us a copy for future editions.

As far as computers go, the three most popular have are the TI 99/4A, the TIMEX-SINCLAIR computers, and the APPLE computers. The AMIGA computer looks like it has great potential for boxing. The TI and TIMEX computers are popular because they are small and compact.

More important, the TI can also play up-to three pure tones, plus a fourth noise tone, simultaneously. Programming the TI for sound is not difficult. Also, its audio output are taken from the rear. Audio output is the DIN pin located at 9 o'clock; it's ground is right beneath it. Since it produces sharp square waves, one should round them off by inserting a 0.1-0.33 uf capacitor across the audio output, or by feeding it into an active filter buffer stage.

The APPLES are popular because they can be easily hooked-up to the APPLE-CAT Modem. This modem is like any other modem, except that it has a few nice features. It can dial numbers and has an auto-answer, like most, but, besides dialing in pulses, it can dial numbers in TOUCH-TONE, and it can receive TOUCH-TONE data! This allows one to use his computer from any phone without a terminal, by simply using TOUCH-TONES instead of a normal carrier. Also, it makes breaking into SPRINT a lot easier. The APPLE-CAT Modem is expensive, about \$250.

Included herein are three popular computer programs for Blue Boxing, which we've derived from 2600, donated by a Ford Prefect. Enjoy.

Continued From P. 12!

CF Boxes can be secreted anywhere (except payphones), but they are primarily secreted on multi-line commercial phone circuits (not inside the actual phones), and are dialed after hours. Commercial phone circuits have these advantages:

(A) High phone charges are less likely to raise suspicions. Many large corporations are ripped-off for \$ Thousands monthly.

(B) Pinpointing suspects is difficult should the CF Box be discovered.

(C) Normal phone use late at night is, in most cases, is non-existent, so accidental discovery is rare. A CF Box was recently shown on an episode of MIAMI VICE.

It should be noted that, with the increased security Bell has implemented against other types of boxing, the CF Box is becoming the box of choice for phreakers.

OTHER BOXES

Other important boxes (I didn't name them Ma'am - just reporting the facts!):

PURPLE BOX: Combines the function of Red and Blue Boxes.

S&M BOX: Combines the function of the Black and Blue Boxes (S&M = Sado-Masochism = Black & Blue).

BEIGE BOX: Any device that can imitate a Model 33 Teletype to a remote computer terminal designed to receive Teletype data.

WHITE BOX: A Touch-Tone key pad (12 keys), or any device that imitates a Touch-Tone key pad.

GREY BOX: Imitates a Touch-Tone pad with 16 keys or with 1633 Hz included.

BROWN BOX: Combines as many other boxes as possible, but with Purple and Grey at the minimum. Because of the Brown Box's complexity, it is usually either generated by a computer or a controller-type circuit. Most Brown Boxes use crystal oscillators to guarantee frequency stability.

YELLOW BOX: A simple 2600 Hz generator. Also called the "Capt. Crunch Whistle" and the "2600 Perfector."

MUTE BOX: Any destination device that makes conversation possible while making Bell think that the called party never answered. The Black Box is the best known Mute Box, but there are also others.

GREEN BOX: Used in conjunction with the Red Box, the called party can use the Green Box to return initial coins to the party calling from a phone booth. Not safe for any calls over three minutes, nor LD calls made thru an ESS.

CLEAR BOX: Used primarily in Canada and thruout rural America, the Clear Box works on "post-pay" type payphones. In these payphones, one pays after the connection is made. Although he can hear the called party, he can't speak to them until he deposits his money. This problem is "cleared up" by inductively coupling into the payphone's circuitry.

SILVER BOX: Better known as the Remote Observation System (REMOBS) or a Lineman's Handset. Sometimes confused with the Beige Box. The Silver Box permits "authorized" telephone employees to dial into private phone lines from anywhere, and then, using an ordinary Touch-Tone phone, tap into a private phone line's receive-only circuitry. Since the mouthpiece is not hooked up, the

tap is totally silent. With a Silver Box, one could silently tap anyone's line.

UK BOX: A Blue Box with United Kingdom tones.

CHEESE BOX: A home-built conference line, or loop-around.

BUG BOX: Any phone bug.

ORANGE BOX: A device, when hooked-up to the phone, displays or records automatically the phone number of the originating phone. This legendary box is rumored to be copied from a similar device used in a special SONY answering machine. We have been unable to verify whether or not such a device actually exists in any off-the-shelf form - including in SONY equipment. If you have any information - schematics, etc. - please write us immediately!

PHONE SCAMS

RIPPING-OFF PAYPHONES

In a publication, it is difficult to explain precisely where and how much of something to apply, particularly when variables exist. Obviously, the more practiced the phreaker is, the more he can accomplish. Not every experiment will lead to success, but some may lead to success far beyond expectations.

Phone boxing is not the only way that payphones are ripped-off! Some other methods:

HUBBLE-BUBBLE

A thin layer of well-chewed bubble gum (syrup or honey) is placed around the edges of a quarter. The quarter is then immediately frozen to harden the gum. Shortly after removal from the fridge, just as the gum is becoming tacky again, the quarter is placed in a payphone. A phone number is dialed that one knows will not be answered. This permits the gum to become more sticky and to adhere to the innards of the phone. The phone is then hung up, and the coin is not returned. Subsequent users of the phone will be unable to obtain coin returns because their coins will stack up behind the gummed-up quarter. Then, the next day, the phreaker returns to the phone. He uses one or more of these methods to break-up the quarter jam to receive a slot machine-like return:

(1) He slams his fist or some other hard object into the body of the phone to shock the quarters loose.

(2) He snakes piano wire into the phone and maneuvers it to pop off the stuck quarter.

(3) He sprays a solvent, such as WD-40, thru the coin slot to dissolve the the gum's adhesive.

Different techniques have been used. It has been reported that, during LD calls, if the quarter jams the coin-sensing relay into the ON position, multiple quarter deposits will be indicated, thus relieving one of using a risky Red Box to simulate coin deposits. This is done by causing the quarter (or slug) to snag onto the vane that activates the relay, then, after substantial credit has been given for the number of "quarters," the jammed quarter is made to release as above if it doesn't fall off by itself. This method has been known to work just by heavily spitting onto quarters. Thus, one could tell the operator, "So that our conversation remains undisturbed, I'm going to deposit this handful of quarters into the phone. Please let me know when they've all been used up and you need more."

A variation of this method is to place the gum into the coin slot. Then, with a penknife, the phreaker works the gum deep inside the phone and out of sight. Subsequent coin deposits will then pick up the gum, and do as before.

Another variation is to use syrup or honey. The syrup or honey container is heated in a pot of boiling water to increase its flow. It is then sucked-up into a syringe heated in the same water. The syringe is insulated. The syrup or honey is then injected into a phone coin slot. As it cools down and evaporates, it becomes sticky as hell. Injecting water into the coin slot will dissolve the syrup or honey and release the stuck coins.

Still another variation is using wads of paper. A half-inch or larger square of stiff paper or index card is folded in half, then with a key or small screw driver, jammed into the phone (bent end first). It may help to dampen (but not soak) the paper first, or to coat it with syrup, honey, wax or gum. Then, coins deposited are jammed by the paper. After a while, the phreaker returns and unjams the phone as described above. If the paper is too large, not even the phreaker will be able to unjam it.

WIRE CROSSING

Another popular method is to cross the green and yellow payphone lines. This is done by using a sharp screwdriver or a carbide glass

PHONE COLOR BOXES

16

drill bit to ream a hole into the plastic light cover used in payphones. A darning needle is then inserted to extract the green and yellow lines. They are switched with each other. When one lifts up the phone and deposits his coin(s), a busy signal is returned. He then hangs up and expects his refund. The refund does not result, but instead, piles up inside the phone. When the phreaker returns, he re-crosses the green and yellow lines, and all coins are then returned at once. Sometimes it takes putting in a dime to trigger the relay to make the return. Phreakers have been known to rip-off phones at \$75+ per click.

Bell is on the look-out for this scam. Consequently, most phreakers take care to only apply it to popular phones on a busy night (ex: Friday, Saturday or holiday), only for a day or so, and never on the same phone twice in a month.

MULTIPLE CLICKS

In parts of the country that have NOT gone ESS, this method appears to work:

The phreaker dials a toll-free LD phone number direct. As soon as he hears a click, he pushes down the hang-up button several times, very quickly, for several seconds. A local operator should come on to the line as this is one method of signaling for operator attention. The phreaker states that he was calling a toll-free number, and that something must have gone wrong because the next thing he knew, he was talking to the operator. At that point, the operator should ask the phreaker for both his phone number and the destination number. The phreaker gives the operator a number other than his, but with the same prefix (not a payphone number) as the origination number. Usually a known non-operating number or one owned by his favorite enemy is provided. The operator then dials the toll-free number from her station. The phreaker then uses his Blue Box to "off" the trunk, and proceed with his normal Blue Box call. Should Bell discover this Blue Box effort, the records will show the phony origination number.

BAD CALL CREDITS

When you make a payphone call and you get the wrong number or the phone phouls up, you are entitled to either the money back from Bell or credit. Phreakers often tell operators that a payphone at such-and-such location and so-and-so number cheated them out of "X" value of coins, and to apply the credit for the current call. Although this scam doesn't always work, it works enough that phreakers still use it. Most operators today will require your name, address, and home phone number to send you a refund. Consequently, this scam is not as popular as before.

THIRD PARTY BILLING

You can bill a payphone call to your home phone. Phreakers often take advantage of this by claiming that they are low in cash (just robbed, etc.), and can't make a call unless billed to their home. They then provide someone elses phone number. Bell operators now ask for personal information to verify that you are the person you claim to be - like what is your Mother's maiden name.

COLLECT CALLS TO PAYPHONES

Calling collect to a payphone is an old scam that doesn't usually work today because payphones are identifiable by their numbers, and operators seldomly accept collect calls to payphones.

PHONE CREDIT CARDS

The most costly and popular phone rip-off is the phone credit card scam. By hook or by crook, phone credit card numbers are found, and, within a short period, they are spread to many people "with connections." The victim may get an enormous phone bill, in some cases, exceeding \$100,000! We go into much greater detail in, CREDIT CARD SCAMS (\$7).

MOUTHPIECE STATIC

The phreaker uses a sharpened screwdriver or other sharpened tool to bore a small hole into the mouthpiece of the payphone (about a quarter inch from the edge). He then inserts one end of a 6" piece of wire into this hole, and touches the other end to a grounded metal object (ex: phone body) creating static noises. The static noises simulate coin deposits and result in free calls. Although this method is very crude, I've heard that it still works!

DISK SERVICE MANUAL II ■ PRINTER & PLOTTER ■ COMPUTER PHREAKING ■

Disk drives MUST be periodically cleaned and lubricated, and repaired as needed. Malfunctions can be devastating in lost programs, data and text; loss of business; upset customers; down time. YOU can maintain, troubleshoot, and repair drives WITHOUT EXPENSIVE OR DELICATE EQUIPMENT OR DIAGNOSTIC SOFTWARE - often in situ and in less time than it takes you to remove, pack, ship, receive, un-pack, re-install, re-configure, and retest drives sent to drive repair shops! Shipping drives is risky! If you want the job done right, on time, and at minimal expense - DO IT YOURSELF! OVER 100 LABELED PHOTOS AND ILLUSTRATIONS OF STANDARD-BUS 5.25", 8" AND MICROFLOPPY DRIVES, AND SPECIAL DRIVES (APPLE, COMMODORE, SONY)!!

Chapter I: GENERAL. Chapter II: OPERATION ADVICE & TIPS. Chapter III: ERROR MESSAGES (and what they mean). Chapter IV: DIAGNOSTICS & TROUBLESHOOTING (how-to-step-by-step). Chapter V: MAINTENANCE. Chapter VI: SPEED ADJUSTMENT. Chapter VII: R-W HEAD ALIGNMENT (includes hysteresis and eccentricity). Chapter VIII: ELECTRONICS & REPAIRS (includes control power/ground system wiring). Chapter IX: MISCELLANEOUS REPAIRS (T00 Sensor, T00 End Stop, Sector Index, Write-Protect, Head Loader, Compliance, Cone Assembly, Spindle Assembly, Module Assembly, Logic Boards, Spindle Motor, Door). Chapter X: DRIVE TEST STATION (Professional Shop Plans). Chapter XI: REPAIR SHOP TECHNIQUES. Chapter XII: DRIVE ANALYSIS SOFTWARE CRITIQUE. Chapter XIII: DRIVE MODIFICATIONS. Appendix A: GLOSSARY. ONLY \$22.

Printers and plotters are costly, with little relationship between cost, quality and capability! **PRINTER & PLOTTER MANUAL** describes:

- (1) The physical specifications, features, and control codes of popular printers and plotters.
- (2) Printer and plotter interfacing, problem areas and how to correct them. Some are hard to interface. Most can be memory-upgraded to save YOU much time and expense.
- (3) Many cost-saving tips and recommendations in the purchase and operation of printers and plotters.
- (4) Circuit diagrams of X-SWITCHERS. Independently switch one/two printers or plotters to one/two computers without disconnecting either. Schematics of Centronics Parallel, RS-232C and 20 ma Current Loop.
- (5) Additional sections devoted to **PRINTER TYPES, PLOTTER TYPES, EXPANDING MEMORY, INTERFACING, ELECTRONIC TYPEWRITERS, RIBBON RE-INKING, SECRETS, PAPER, PATCHING SOFTWARE, SPEED RATINGS, BUYING STRATEGY, and RS-232C PROTOCOLS.**
- (6) BUFFERS, SPOOLERS, MEMORY UPGRADES, ELECTROGRAPHIC, TRACTOR-FEED, DIE AND PANEL SWITCHES, DOT-MATRIX, DAISY WHEEL LINK JET, LASER, FLAT-BED, ROLLER-BED, DRUM, WORDPROCESSING, DATAPROCESSING, CAD/CAM, TIME-OUT PROBLEM, GRAPHICS TABLET, CALLIGRAPHY, HS TYPESETTING, ADVERTISING, PUBLICATION LAYOUTS, etc.

Over 100 printer- and plotter-related terms defined, including abbreviations, control codes, and interface terms.

- (7) Cleaning, lubricating, maintaining, and repairing printers and plotters, with actual examples.

Comprehensive and exhaustive - many illustrations and photographs - ONLY \$15.

According to the FBI, less than 5% of all DISCOVERED computer crimes result in conviction! Computer crime, or "Phreaking" costs \$ Billions per year, and is clearly one of the most dangerous - yet most profitable and least risky - of all crimes! **COMPUTER PHREAKING** describes in detail:

- (1) Dozens of computer crime methods. Schemes include: Input Transaction Many, version, File Alteration & Substitution, Unauthorized Software Modification, Code Busting, Wiretapping, Electronic Trespass, etc. Many actual examples - detailed case history based upon actual court records of a major group! Why/how Government, business and financial institutions are easily victimized by savvy Phreaks!
- (2) Numerous countermeasure, protection and security schemes - passwords to public key encryption methods. State-of-the-art techniques. Foil even the sharpest Phreaks!
- (3) Definitions of popular computer crime terms, including PIRACY, TROJAN HORSE, LOGIC BOMB, TRAPDOOR, GODFATHER, MUTANT ZOMBIE BODY, SNATCHER, SILENT ALARM, CHEESEBOX, CANDYMAN, CODE 10, etc. Learn how to become a computer crime fighter! Comprehensive, illustrated, frank. ONLY \$15.

DISK DRIVE TUTORIAL II ■

The detailed theory and practical facts of floppy drives, diskettes, FDCs, interfacing, formatting, and disk-stored software. A must for the Student, Programmer, and Computer Shopper (save \$\$\$)! Relates to drives of every manufacture, and used in IBM, APPLE, TANDY, COMMODORE, KAYPRO, TI, HP, NORTH STAR, ATARI, DEC, etc. systems. DOZENS OF LABELED PHOTOS AND ILLUSTRATIONS.

Chapter I: GENERAL. Chapter II: DISK DRIVES. Chapter III: DISKETTES. Chapter IV: INTERFACING. Chapter V: FORMATTING. Chapter VI: SOFTWARE (compatibility and protection). Chapter VII: RECOMMENDATIONS. Appendix A: ADDRESSES. Appendix B: GLOSSARY. ONLY \$17.

COPIER MANUAL ■

The total cost of a modern photocopier can exceed that of a new car! Yet, copier prices and brand names have little to do with features and quality! Until **COPIER MANUAL**, almost nothing was available for you to compare copiers for features, quality and price. Modern copiers are dropping in prices, and have substantially increased features and quality. **COPIER MANUAL** describes in detail:

- (1) Evaluations of dozens of features, and prices of over 100 popular modern copiers manufactured and/or sold by A.B. DICK, CANON, GISTNER, IBM, MINOLTA, MITA, MONROE, PANASONIC, PETNEY BOWES, RICOH, ROYAL, SANYO, SAVIN, SHARP, 3M, TOSHIBA, and XEROX!! Also includes evaluations of dozens of quality factors of many of these copiers exhaustively tested by us.
- (2) Our evaluations of each major copier manufacturer, which ones we recommend, and their addresses. An in-depth evaluation - advantages and disadvantages - of the copier we recommend as the best buy for an office copier.
- (3) Dozens of little known facts and tips on copier selection and operation. How to make substantial savings on purchases, maintenance, repairs and supplies. How to extend copier and drum life. Where to get cheaper supplies - what you can and cannot recycle. Copier myths debunked!
- (4) The optimum combination of paper and ink color to protect YOUR copyrighted publications and classified data from unauthorized use. How to copyright publications.

Frank, comprehensive and exhaustive! Dozens of illustrations, photographs, and tables. Designed to save YOU \$ Thousands. ONLY \$15.

COMPUTER SECURITY ■

Computer crime is rampant and increasing! Annual losses are \$ Billions - plus devastating losses in privacy, personal security, etc.! **DON'T BE VULNERABLE!**

We developed many versatile, simple-to-apply, virtually impossible-to-defeat, computer security techniques. These include, but go far beyond, passwords and ciphers. No hardware or ROM mods required.

Included are invulnerable BASIC cipher algorithms (encryption and decryption); BASIC program for computing, testing multikeys; cipher program design techniques; how to use zaps to protect disk files from unauthorized access; clever concealment techniques; secure operations procedures; Review of security books - more!

\$1,000 CONTEST: WE WILL AWARD \$1,000 to the FIRST CONTESTANT WHO CORRECTLY DECIPHERS OUR 25,000+ CHARACTER CIPHERTEXT!! Now that we've polished off the lightweights, it's time for YOU to show us your stuff! Not a "public key", DES or "one-time pad" cipher. Included are details, contest rules, and many hints and clues. Complete descriptions and illustrations. ONLY \$25.

STOCKPRO II ■

An effective, yet unique and unconventional method to select common stocks! Multiple applications demonstrated that stocks chosen by **STOCKPRO** subsequently increased in value by an average of 31% to 211% per year!! **STOCKPRO II** is upgraded with increased analytic powers. Use the tried and statistical and intuitive approach of **STOCKPRO II** to outsmart the legions of Wall Street eggheads! Completely described and illustrated. Written in straightforward MICROSOFT BASIC.

ONLY \$15 for all Documentation (includes listing). ONLY \$50 for Diskette + all Documentation.

SUPER RE-INKING METHOD! ■

New printer/typewriter cartridge ribbons are costly, and yet may produce less than 5 hours of quality copy! And are an inconvenience to order - **WHEN YOU CAN FIND THEM!** Now, you can re-ink your own cloth ribbons to last about 10 hours of quality use for about 50 cents and 10 minutes of effort per ribbon. Not any ink will do! We developed the right combination of clay-free ink and carrier - both commonly and inexpensively available from stores in black and 4 colors. Includes complete plans for your own el cheapo motor-driven re-inker. Completely described and illustrated. **STOP WASTING MONEY ON RIBBONS!! ONLY \$7.**

By John Williams, MSEE, former CS Professor, NMSU We pay all U.S. shipping! (12%, \$3 min. foreign orders). Please allow 4-6 weeks for check-paid orders, else 2-3 weeks. Quantity Buyers welcomed - Substantial quantity discounts. Custom editions for quantity orders! **PLEASE ORDER TODAY! FREE CATALOG** for all orders over \$20 (else \$1).

Consumertronics Co. ALAMOGORDO, NM 88310
2011 CRESCENT DR., P. O. DRAWER 537

OUR SUPER-SURVIVAL CATALOG DESCRIBES ALL OF OUR CONTROVERSIAL FOR-YOUR-EYES-ONLY PUBLICATIONS, PLEASE SEND \$1 FOR IT!

PHONE COLOR BOX ADDENDUM

COPYRIGHT © 1988, JOHN J. WILLIAMS and FAMILY. ABSOLUTELY ALL RIGHTS RESERVED
By: John J. Williams, MSEE --- CONSUMERTRONICS CO., P.O. Drawer 537, Alamogordo, NM 88310

INTRODUCTION

PHONE COLOR BOXES is one of CONSUMERTRONICS most popular publications. Because of the demand and interest in these and other phone circuits, we massively improved it with this addendum. **THIS ADDENDUM IS PROVIDED FOR EDUCATIONAL PURPOSES ONLY.** No illegal use is recommended or implied. As well as much additional info. on phone color boxes, we also included plans for dozens of very useful and legit phone circuits. Enjoy.

Our publications largely depend upon reader contributions. CONSUMERTRONICS is considered to be THE NATIONAL CLEARINGHOUSE FOR SURVIVAL INFORMATION (since 1971). To contribute color box and other circuits and info., please write me at:

CONSUMERTRONICS

2011 Crescent Dr., P.O. Drawer 537
Alamogordo, NM 88310

Please don't call - we are always swamped here. If you require compensation for your contribution, let us know in advance. We accept anonymous contributions, and confidentiality is guaranteed.

CUSTOMIZED DESIGNS

While reading this manual, you are bound to say, "I sure could use something just like that!" We can now build any of these circuits, or any combination of them, or any other phone-related circuit for you on a customized basis. Confidentiality is 100% guaranteed. We build all devices with the clear understanding that buyers are totally responsible for all of their actual uses, and that no devices are provided for the intention of any illegal use whatsoever. The devices we build are in sturdy boxes, come with documentation, and are very simple for you to install and use. Only these steps are required:

- (1) Unplug the phone line from the back or underside of any home/business phone, and plug in the device's modular plug.
- (2) Plug in the line's modular plug into the device's modular jack.
- (3) Then switch the device ON. If the device requires a battery(s), we will ship it with a new alkaline battery(s) installed.
- (4) Some circuits come with extra controls and/or connectors. Their uses will be explained in the accompanying documentation.

For us to provide you a specific estimate:

- (1) Send us a list of the phone circuits you wish to have made for you. A "device" consists of one or more circuits mounted in the same box. You can combine 1-10 circuits into any device as you wish.
- (2) Include a non-refundable research fee of \$5 for each circuit you are interested in, \$10 minimum for each device.
- (3) Within four weeks, we will return to you an estimate of what we will charge you for each device you specify.
- (4) We require, in advance, a non-refundable downpayment of at least 1/3 of the estimated cost for each device you ask us to build for you. Upon completion of your project (which usually takes less than six weeks), we will ship the device(s) to you, COD, for the 2/3 balance. CONSUMERTRONICS reserves all patent rights to its inventions.

WHICH BOXES WORK & WHERE?

Since publishing PHONE COLOR BOXES, we have been frequently asked, "which boxes work and where do they work (best)?" Without hiring dozens of employees and sending them all over the U.S. and Canada, we can seldomly provide an answer to that type of question. Things constantly change. We get reports from all over, but compared to the number of phone systems, the input is very small, spotty, often vague or contradictory, and can't be substantiated or correlated.

It is true that since MOST (but not all) areas have converted to ESS (Electronic Switching System), Blue and Black Boxes are now practically unusable, and that all boxing is much less certain or safe. Electronic switching offices that use the CCIS (Common Channel Interf-

face Signaling), cannot be Blue Boxed because, under CCIS, all signaling is done using separate data lines that cannot be accessed by the phreaker. This method is called out-of-band signaling. The old, in-band signaling method sent the control signals along the voice lines and thus could be Blue Boxed.

Standard Black Boxes cannot be used under ESS because there is no direct connection made until the receiver is lifted and billing begins. Thus, Ma Bell has a record it can analyze even if it could be tricked into recognizing a pseudo hang-up as a real hang-up without following it automatically with a disconnect.

In fact, under ESS, standard infinity bugs are no longer useful because of this fact, and fact that the ring back you hear is an artificial one produced by the system and not the one actually being delivered to the called number, and there are usually significant timing differences. We understand that a more sophisticated infinity bug now exists that works with ESS. This device works by blocking the phone ring between the phone line and called phone. The bug then "answers" the phone (goes off-hook), so that ESS will switch the tones generated at the calling end thru. If tones are detected, the infinity bug then switches to the eavesdropping mode. If not, then it simulates the phone ring until either the caller hangs up, or the phone is normally answered (it then drops out). The design of this box (the Bug Box) will appear in our upcoming TELEPHONE RECORDER INTERFACES II. We welcome ideas!

Boxing has become much more dangerous because much greater and faster record keeping and detection methods have been implemented, and the various carriers are increasingly sharing security information. Even if you Black Boxed a cross-bar system, teleco computers can now quickly detect the characteristic excessive ring period of Black Boxing (even if you filter out the ring at the called end). Under ESS, every single digit dialed is recorded by computer - even for local, service, operator and directory assistance calls! Even tones generated in the middle of phone calls! In fact, newer versions of ESS are designed to silently alert security when any "foreign" tones are detected - local or long distance! Under ESS, call tracing is sophisticated and immediate.

Red Boxing is also is much less safe to perform. Most pay phones now require that the coin physically trips a microswitch inside the pay phone. This can be overcome by depositing the first required coin, then boxing the remainder. Also, the coin's pulse shape is now more critically analyzed, and many systems recognize pure square waves and sinewaves as boxed tones. The required pulse shape is trapezoidal, but clipped sine waves are almost always accepted.

Don't ever assume that anything you say over the phone is private and confidential! This is why we don't like to receive "sensitive" phone calls. At least two Government agencies (NSA and DEA) are known to use supercomputers to routinely monitor phone conversations transmitted via microwave (virtually all long distance calls and many local calls out of a central office are now microwaved). Each conversation is temporarily recorded and searched for trigger words, terms and phrases. If they are found, the conversation is permanently recorded, along with the called/calling phone numbers, for later analysis and disposition.

DIVERTERS

A DIVERTER is the most common type of Call Forwarding. It's used particularly by small business people and professionals (ex: doctors, psychiatrists, dentists, plumbers, real estate agents) to automatically route office calls to their home after hours. These people are almost always listed in the Yellow Pages.

Phreakers love diverters because they can use them to place free long distance calls. Diverters are used for calls that can't be made thru extenders. These include international calls and Alliance Teleconferencing calls.

The phreaker calls a local number he suspects uses a diverter, after 7 PM. He listens for multiple clicks BEFORE ringing starts, which are a

give-away that the call was diverted (multiple clicks AFTER ringing starts usually mean that more than one extension was lifted). And if the call is answered at all by a relevant person (not a service person or answering service/machine), the subscriber is working very late, operates his business from his home (which can usually be ruled out by his office address), or the call was diverted. When the phone is answered, the phreaker then claims wrong number or some other dumb excuse. When the subscriber hangs-up there is often a few seconds of his own dial tone played out. When that dial tone starts, the phreaker then quickly dials out the phone number of real interest to him. The subscriber is later billed for the call.

There are other types of call forwarding. The DOD Fraud Hotline was one. PBXs (Private Branch Exchanges) are another. Sometimes when a PBX call is disconnected, it leaves the phreaker with a dial tone INSIDE the PBX. PBXs are popular with larger companies. After talking to an employee, the phreaker waits until he hangs up. Or he calls the PBX after hours and hopes that he is left inside the PBX once the recording is over with.

Once the phreaker has the local dial tone, he can then dial to the first local access ports (switches) of one of the common carriers (AT&T, US Sprint, MCI, Allnet, RCI). When the local port answers, it places a carrier (system) dial tone on the line. The phreaker then punches in the access code, area code and number of the next target port, preferably located in a large, distant city. When the second port answers with its dial tone, the phreaker punches in the access code, area code and number of the next target port. This process repeats itself as many times as desired to help obliterate the trail back to the phreaker. Finally, the phreaker dials his destination number.

COLOR BOX DEFINITIONS

There is confusion about the definitions of the lesser known color boxes. We don't claim to be an authority on color box definitions. We published those definitions provided to us by others. Color box definitions given in the Spring 1988 issue of 2600 MAGAZINE and from other sources include:

SILVER BOX: Able to simulate the DTMF (Dual Tone, Multi-Freq.) and have the availability to generate 1633 Hz. Tones are used on the Auto-voice network (military phone system). This definition is the same as what we call the GREY BOX. I have been informed that the Silver Box has nothing to do with either REMOBS or Lineman's Handsets.

CLEAR BOX: Allows calls to be placed from the new private payphones that block the phone's mike until a coin is deposited. But by using an impedance tap type of device, the speech of the caller can be electronically placed in the earpiece and the conversation can proceed normally. This definition differs from the implementation method than what we stated.

BLOTTO BOX: Combination of Blue, Red and Black Box. New term.

CHEESE BOX: Allows for a call to be placed to one location and then transferred to another on a different line than the original number called. Used to hide actual location of the caller from traces by separating and isolating the call from the other line. This definition clarifies ours. One source stated that an effective Cheese Box method requires subscription to a Call Forwarding service, Red Box tones and the number to your Prefix Intercept Operator (PIO). You then use your CF to forward all phone calls to the PIO. This will set up your phone as a payphone, and it will wait for the quarter sound, which is produced by the Red Box.

TRON BOX: Allows one to reduce the electric company's meter registration of his energy usage while he uses the same energy, by placing capacitors across the 120 VAC power lines. The Tron Box is based upon the theory that by correcting the power factor load-side you somehow fool your meter into either slowing down or reversing. First, to avoid confusion, any term with the word "Box" in it should be relegated to phone boxing only. Second, the electrolytic capacitors specified by the Tron Box design are very expensive, age fast, and have been known to explode. Third, this stale idea is circa 1928! At best, it just makes your meter run more efficiently while costing you the same (plus the added power dissipated by the capacitor bank). At worse, it so adversely affects the magnetization current of induction motors, that you get motor stall and burn-out. CONSUMERTRONICS publishes some Dyn-O-Mite publications on electric, natural gas, gasoline, diesel fuel and water metering. See our SUPER-SURVIVAL CATALOG (\$2) for more info.

PHONE COLOR BOX ADDENDUM 2



PHONE COLOR BOXES

NEW - MORE INFO. ON COLOR BOXES - PLUS MANY MORE USEFUL PHONE CIRCUIT PLANS! Designed by Phone Phreakers: 15 Phone Color Boxes, described Owners Circuits, Programs, Plus Call Forwarding, Conferencing, Phreak History, more! For posting \$20

HIGH VOLTAGE DEVICES

NEW - COMPLETELY REWRITTEN - MANY MORE PLANS! HV Devices, Shot Gun, Taser, Prod, Game, Underhills Zapper, Jammer, Flasher, Blaster, Jacobs Ladder, Plasma, and Van de Graaff Gens. Ferris Wheel, Tangle Counter, Ozonizer, Fish Shaver, Prod Killer, Plus Stimulator Devices. SHOCKING! \$20

ELECTROMAGNETIC BRAINBLASTER

Plans for powerful ELECTROMAGNETIC WEAPONS and LAB DEVICES. Optimum circuits, frequencies, waveforms, intensities. Comprehensive Mind Boggling! \$20

RADIONICS MANUAL

Once dismissed as quackery, some electromagnetic and electronic Therapies are now FDA Approved. History, descriptions, plans (dozens) circuits, availability of RADIONICS DEVICES from early tube type to modern IC. Comprehensive. Illustrations and eye opening! \$20

SECRET & SURVIVAL RADIO

Comprehensive manual on optimum survival and security radio equipment, methods, frequency allocations, and voice data scrambling, including: Includes: small receivers/transmitters, telemetry antenna optimizations, remote monitoring, control, security, surveillance, and ultrasonic, fiberoptic, infrared, comms. 70+ Circuits, Tables \$20

VORTEX GENERATOR

Heat, cool, with Simple, Amazing 3-Port Device. Uses no moving parts, electricity fossil fuel, liquid or from. Guaranteed Scientifically Sound. Plans \$7

TV DECODERS/ CONVERTERS

Plans for several TV Decoders and Converters. Plus Satellite TV components purchase and use tips. Tutorial \$7

PHONE RECORDER INTERFACES

Plans for undetectable (ultra-hi input impedance) undetectable TELERECORDER to record phone conversations. Also monitors for bugs and taps. Plus simple FM transmitter plans. Plus ear-piercing SHRIEK CIRCUIT. Plans \$7

STEALTH TECHNOLOGY

Error rates of police radars are 10%-20%! One speeding ticket - even if it's error - can result in insurance cancellations, or \$100s in rate increases! Describes every known material and method used to reflect and absorb radar signals and argument, theory and theory to fight radar tickets. Includes radar detector, and jammer designs, and radar theory with emphasis on error modes. \$15

THE "GOLDFINGER"

Metal detector finds GOLD, SILVER, PLATINUM, COPPER, ALUMINUM. Rejects all ferromagnetic objects made of iron or nickel. Simple circuit. Plans \$7

THE "SILKWOOD"

Small, simple, (2-10); effective Radiation Detector. No high voltage, heavy, special batteries, or special tubes. Radiation is everywhere! Protect your health! Plans \$7

KW-HR METERS

How electric energy meters work. Calibration, many error modes. ANSI Standards Demand Meters. Pole Meters Polyphase Meters meter creep, overload drop \$15

POOR MAN'S SUPER LASER

Home find Laser Plans, used in intrusion systems, auditor's targeting, precise optical alignment, stereography, signaling and commo, strobbing, holography, science projects. etc. Includes a list of dozens of sources for the tuby rods and associated parts \$7

TECHNICAL RESEARCH SERVICES

200+ electronic and computer design articles in database accessed by little, subject Digital, up, IC, analog, hybrid, nanograph, software. Provide us keys, we return listing. \$25 non-refundable search fee. 11-20 keywords (phrases). Saves you \$55 and more in R&D. Great educational tool!

By John Williams, former Senior Engineer (Lockheed) CIS Professor (MMSU) FREE CATALOG with Order (see \$2) Please add \$2 and USA. Catalogs, COOs, Credit Cards are \$2 extra. VISA, MASTERCARD. All items are in stock. Personal returns and payments only. Satisfaction Guaranteed. Please Order Hours: Mon-Sat 7AM-7PM MST (505-434-0234).

DISK SERVICE MANUAL

Maintain, Troubleshoot, Repair, Adjust, Align Drives without special equipment or software. \$25/3.5"/8" IBM-PC/XT/AT, Compatible, Apple, Commodore, Kaypro, Tandy, Epson, Atari, TI, HP, DEC, etc. Systems 12 Chapters, 100+ Photos, Figures. All drives need servicing. Save \$\$\$ \$20

DISK DRIVE TUTORIAL

Theory and practical facts on Drives, Disks, FDCs, Formatting, Interfacing, Software Protection. Same Drive Types as above. Seven Chapters, many Photos, Figures, Tips \$15

PRINTER & PLOTTER MANUAL

Types, Descriptions, Specs, and 100+ interfaces (Parallel, Serial) Detailed Plans of X-Switches, Buffers, and Serial-to-Parallel and Parallel-to-Serial. Hardware Devices, Repair, Maintain, Many Buy Like Service Tips, Figures \$15

SUPER RE-INKING METHOD

Re-ink with Ribbons for about 50 cents and 10 minutes each. Plans for EI Cheong Motor-Driven Re-inker. Commonly used ink (5 colors) and carrier described \$7

COMPUTER PHREAKING

Dozens of Computer Crime and Abuse Methods, and Countermeasures. How systems are penetrated. BBS, Arpa, Password Details, EMI, Eavesdropping (TEMPEST), Van Eck Methods: Crosstalk Amps, 200 Phreak-Term Glossary \$15

BEYOND VAN ECK PHREAKING

BY POPULAR DEMAND!! Eavesdropping on VDT video signals using an ordinary TV. Ranges up to 1,000 meters! How it's done and countermeasures. Completely described. Also legal Van Eck uses. Dozen Figures (mostly Schematics) and Tables. AN ABSOLUTE MUST FOR EVERYONE CONCERNED ABOUT COMPUTER SECURITY \$20

ABSOLUTE COMPUTER SECURITY

Dozens of simple, versatile, secure Computer Security methods and tips. Plus our Invulnerable Cipher Program in BAS, COM, Source Code! Plus \$7,000 CIPHER CONTEST rules with 25-K Char. Cipher Text. Manual - \$15 Manual + Disk* - \$25

CRYPTANALYSIS TECHNIQUES

3 Powerful Menu-Driven Crypto Programs in BAS, COM, Source Code to Analyze, Decrypt "Secure" Ciphertexts. Examples. Recommended in the prestigious COMPUTERS & SECURITY (Vol. 6, No. 6, P. 453) Manual - \$15 Manual + Disk* - \$25

AUTOMATIC TELLER MACHINES

ATM Crimes, Abuses, Security, Vulnerabilities. 100 methods described - from Reg. E to Cipher. Case histories, law, countermeasures. Detailed Security Checklist. Photos, Figures. ATMs may be hazardous to your wealth \$20

ATM ADDENDUM: New Dyn-O-Mite Text, Photos, Figures \$20 Both Manuals \$30

THE ASSEMBLY LANGUAGE DEVELOPMENT SYSTEM

ASM.COM: Powerful program for creating/editing Assembly Language Source Code. Like a sophisticated wordprocessor but with many unique and powerful features for AL programming.

EXE2DATA.COM: Converts EXE, COM, BIN files into BASIC DATA statements, pre-loaded with needed variables. EXE2BIN not required! Many features.

TUTORIAL: On how to develop and integrate AL Routines into BASIC and Compiled-BASIC programs. Also discusses C, FORTRAN, and PASCAL. Increases speed up to 100 times! Saves up to 90% of memory!

Includes Help and other text files. Disk* - \$25

INTEGRATED SOFTWARE

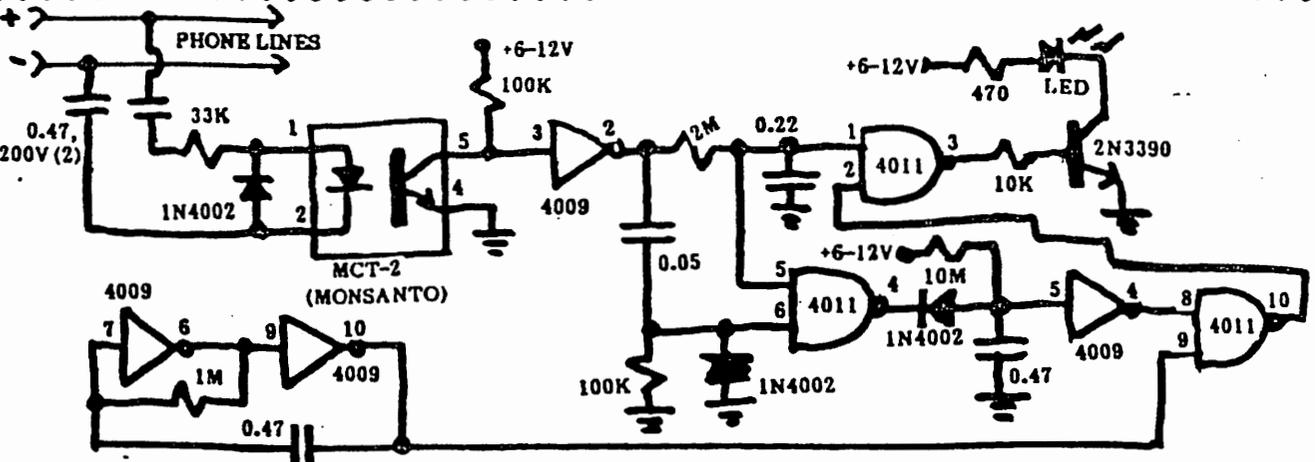
Four powerful, sophisticated, versatile, menu-driven, compatible Programs: WORDPROCESSOR/TYPESSETTER, DATA PROCESSOR, SPREADSHEET, and BASIC PROGRAM PROCESSOR! Plus 100+ K of Help, DOC and template files. Plus both of our catalogs on disk. INCLUDES HEAVILY ANNOTATED SOURCE CODE! Ten Disks* A super good bargain! \$25

*Disk Software Supports PCDOs, MSDOs, PS/2, Mono, Hi-Res, CGA, EGA, VGA, 325", 35", hard (specify your floppy drive size)

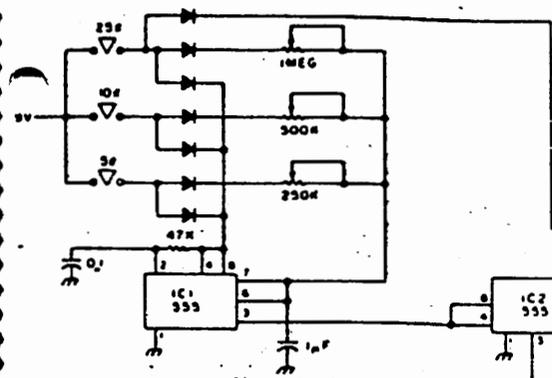
CONSUMERTRONICS
2011 CRESCENT DR., P.O. DRAWER 537
ALAMOGORDO, NM 88310

MORE PHONE BOX CIRCUITS

Reader contributions of additional phone color boxes:

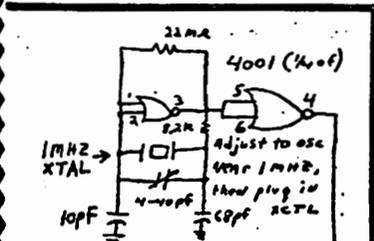
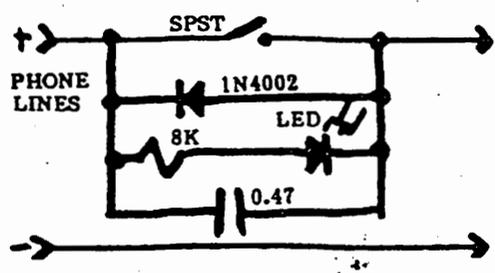


PHONE STATUS INDICATOR: This circuit monitors phone status with an LED. The LED is OFF for on-hook, flashing for ringing, and ON for dialing and off-hook.

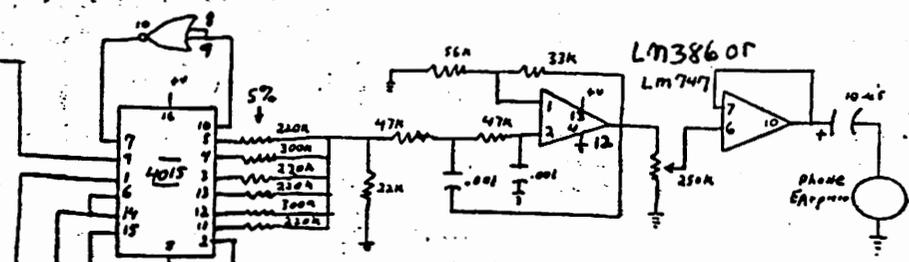
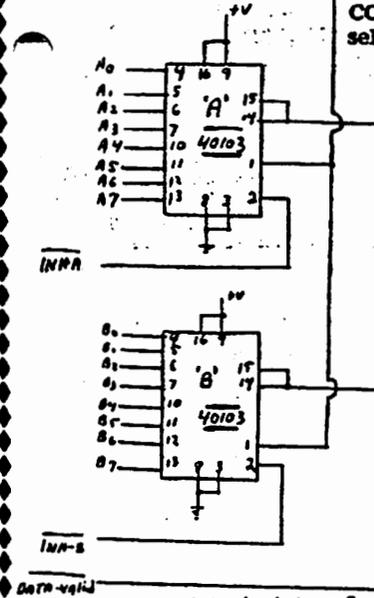


ANOTHER RED BOX: IC1 generates the proper burst while IC2 generates the required rate and duration tone for each burst.

ANOTHER BLACK BOX: This one is supposed to work best in Great Britain. Usually good for at least 3 minutes of phone use. The SPST is opened after the rings start but before the call is answered. If the call is from an operator, payphone, or you wish to make an outgoing call, close the switch.



COMPUTERIZED GREEN & BROWN BOX: This nifty circuit lends itself to μP and μC control of the desired tones.

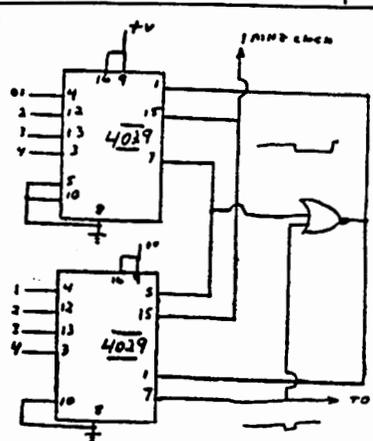


Pin #s shown don't reflect pin locations.

FIG. 1

2600	00101111
3200	00100110
700	10110001
900	10001010
1100	01110001
1300	01011111
1500	01010010
1700	01001000

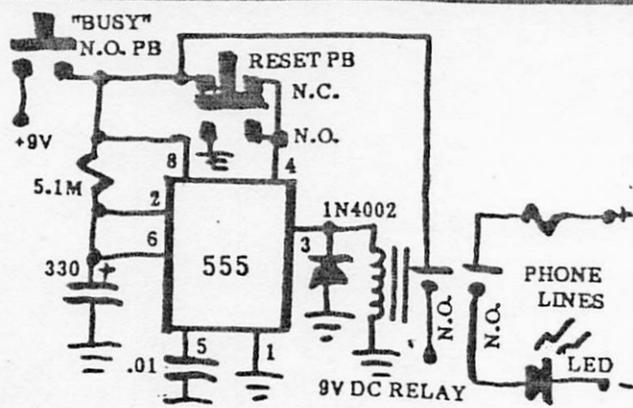
Refer to table 1 for input words
 eg, 700Hz = 10110001
 $Freq = 10^6 / 8 * (N+1)$
 $N = (10^6 / 8 * Freq) - 1$
 code = binary value of N
 N is base 10 value of code



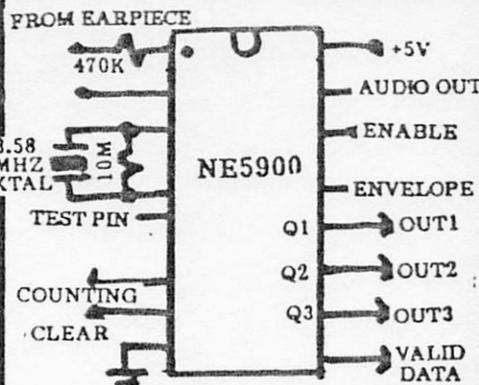
Substitutes for 2 40103
 INPUT - 4, 11, 13
 N.C. - 6, 11, 14, 2

MISCELLANEOUS CIRCUITS

These phone circuits perform a variety of other crucial functions:



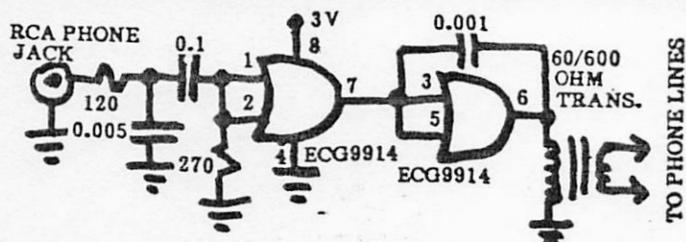
"BUSY" PHONE CIRCUIT: There are certain times that you don't want to answer the phone, while, at the same time, you don't want to be bothered by incessant ringing or give the impression that you are out. You could put the phone off-hook, but then you get those irritating buzzing sounds and "please hang up" messages, and anyone calling you may be told that your phone is out-of-order. This simple circuit makes your phone act like it's busy. You hit the "Busy" PB when you don't want to be bothered, and the Reset PB when you are again available. Simple! It's also very useful to mislead burglars casing your place, to discourage harassing and other unpleasant phone calls, to reserve the phone for you so that when you need it someone else won't be using it, and to assure an undisturbed rest.



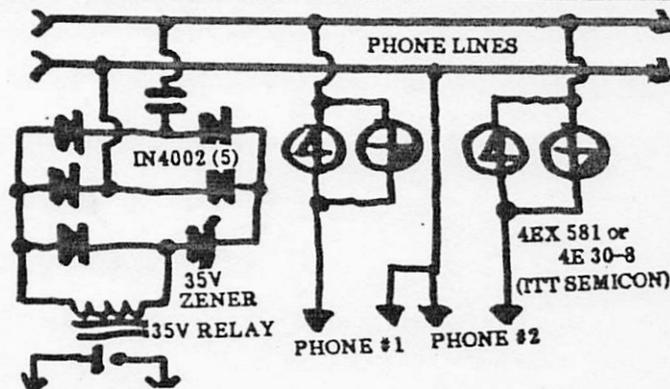
CALL PROGRESS DETECTOR: This circuit is used in conjunction with color boxes, Touchtone keypads, auto-dialers, modems, remote controllers and alarms to determine when the phone is either ringing/busy or off-hook. When the off-hook condition is detected, the data/recorded message is then transmitted. This circuit is connected directly to the input leads of the phone's earpiece. Note that the 470K resistor is critical because it's used in the internal bandpass filter. OUT1 is high for ringing, OUT2 for busy, and OUT3 for reorder. OUT1-3 are low for dial tone and high for overflow (excessive noise level or talking). The Valid Data output is high when the chip detects the right off-hook conditions for data transfer.

Although the freqs. used for dial tone, ringing, busy and reorder (depending upon equipment), their ON/OFF durations are uniform. Dialtone is a continuous tone pair. Ring is ON for two seconds and OFF for four. Busy is ON for a 0.5 second and OFF for a 0.5 second. Reorder (a phone company supervisory function) is ON for 0.2 seconds and OFF for 0.3 seconds.

This circuit uses a stock color TV crystal (3.58 MHz). To initiate the call progress detector, you temporarily ground Clear. Other pins of importance are the Envelope, Enable, Test, Analog Out and Counting. The Envelope pin lets you detect and switch on oddball responses (useful for demon and wargames dialers). The Enable pin lets you turn ON/OFF OUT1-3 and Envelope, and is grounded for ON. The Test pin is used only for testing only, else ground it. The Analog Out pin produces a filtered analog signal and can be used for remote surveillance. The Counting pin lets you count the duration of the try for recycling the Clear.



PHONE LINE INPUT MATCHER: Music sounds so poorly over the phone because, in most cases, the music generator is poorly matched to the phone circuit. Same with that color box you may have been using (shame on you!). Phone lines are 600 ohm. The required transformer (shown) is a 60 ohm/600 ohm one, but any 1:10 audio transformer with 40-75 ohm input works well. Also, if the ratio exceeds 1:10, load the output with a parallel 10K, 20-turn pot. and tune it for the best sound. The ECGs are CMOS AND gates operated in their linear (amplifier) region. Conventional AND, NAND, BUFFER and INVERTER CMOS gates will also work (TTL doesn't work). This circuit also helps smooth out harsh square-wave tones produced by the typical cheap 555 color box, and it is similar to output circuitry used in modems. So, the next time you call your Aunt Mildred in Waco for a recital she can now truly appreciate how bad your voice really is.

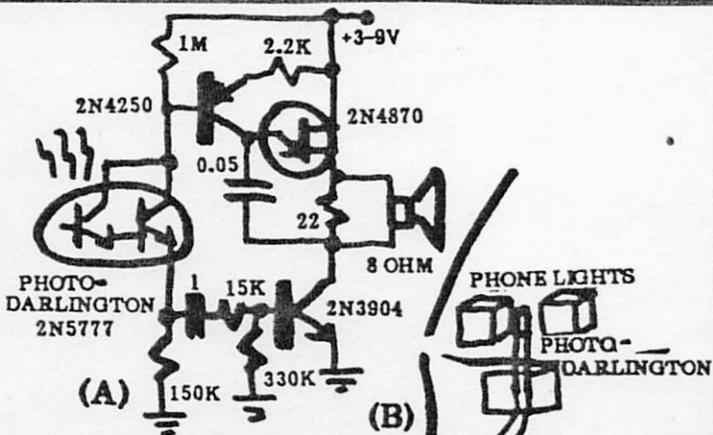


FIRST-PHONE-LIFTED PRIORITY: It's annoying to have six extensions and, every time you get a phone call, every member of your home/business goes thru that same, tired ritual of lifting and replacing phone extensions. Or rudely dialing out when your engrossed in a conversation with your in-laws. With this circuit, once one extension is lifted, all the other extensions are automatically disconnected. This circuit also improves security because bug/extension eavesdroppers are locked out. This also eliminates the problem of having extension bells ding all over the place when any extension dials out.

The trigger diodes used have a breakdown voltage of 33V. The diodes on the first extension lifted thus conduct. Upon lifting the receiver, the line voltage drops to 5 volts, preventing the diodes on the other extensions from conducting until the off-hook extension is hung up.

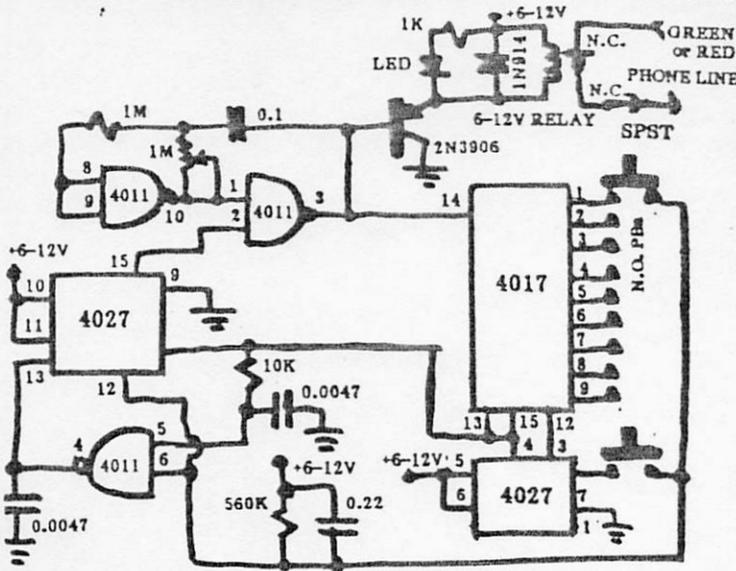
Using this method, a practically unlimited number of extensions can be used with no interference between extensions. In fact, several extensions can share the same diode interfacing. This allows you to wire your extension to one set of diodes and all other extensions to another set so you don't have to worry about unknown and subsequent connections installed to bypass this security.

The circuit part on the left is used in lieu of the internal ringer (which are disconnected) for a distributed ringer (alarm) system.



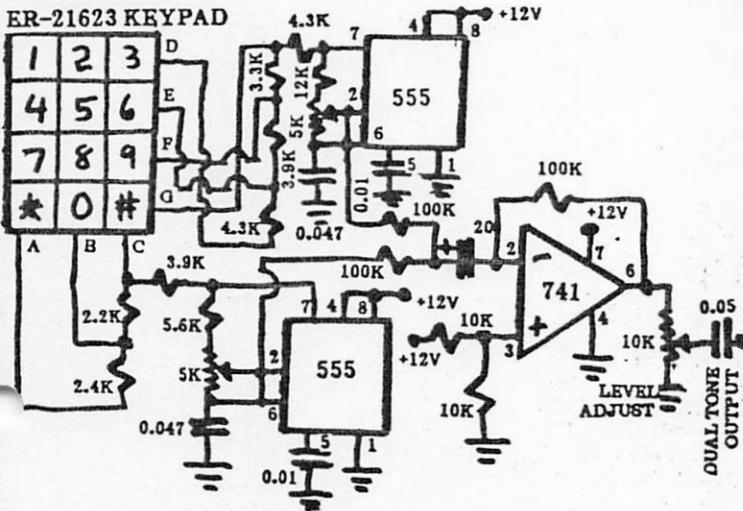
PHONE LIGHT MONITOR: This circuit is used to detect if a phone button (or other) light is ON and to buzz whenever that occurs. No hard connection is made to the phone.

PHONE COLOR BOX ADDENDUM

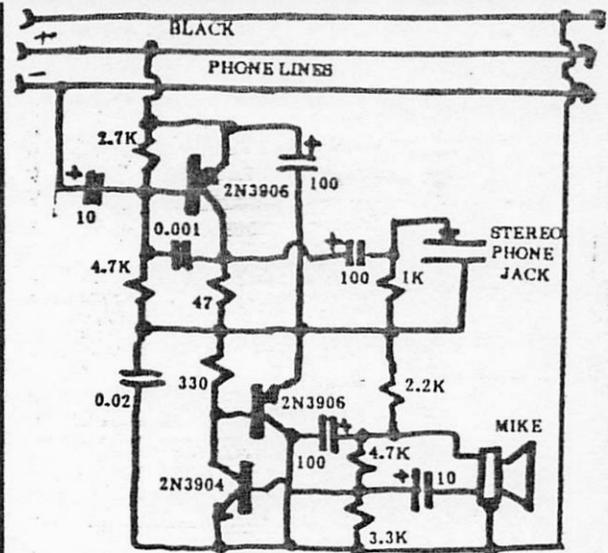


KEYBOARD/COMPUTER INTERFACE FOR AUTO DIALING: This circuit uses a calculator (non-matrix type) keypad or computer or controller input to automatically rotary-dial phone numbers. Opening the NC SPST switch is equivalent to going on-hook, which permits you to start a new call. The LED is used to indicate that the number is being correctly dialed. For computer use, the PBs can be replaced with analog switches (ex: 4016, 4066) that are controlled by the computer's data/address lines.

CHROMERICS ER-21623 KEYPAD

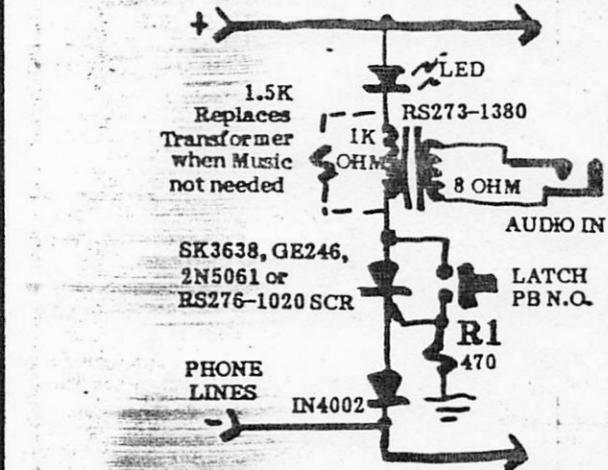


TOUCHTONE ENCODER: This circuit produces the required dual tones used by Touchtone phones. Each 555 produces a tone depending upon which button is pressed on the matrix keypad. The two tones are mixed at the 741 inverted input and amplified. This well-known circuit is commonly modified for color box uses. To do that, the resistors in the resistor ladders to both 555s are changed to duplicate color box freqs.

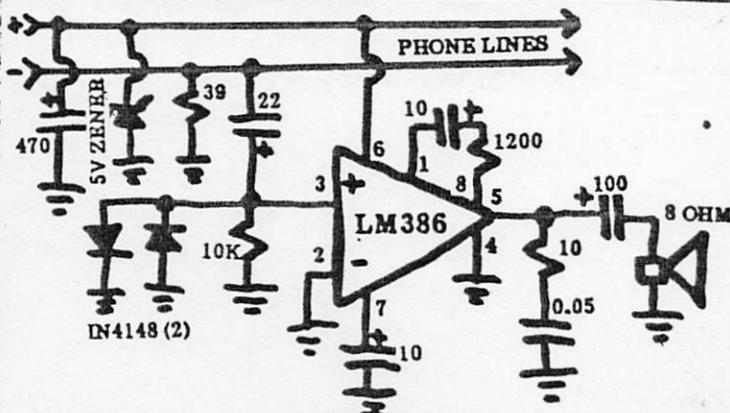


HANDS-OFF PHONE CIRCUIT: This is an excellent alternative to a Speakerphone. It uses stereo earphones and an electret condenser mike.

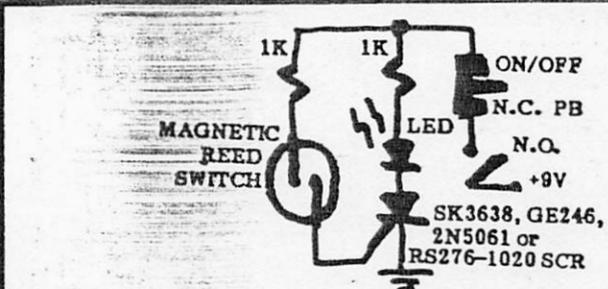
CONSUMERTRONICS
2011 Crescent Dr., P.O. Drawer 537
Alamogordo, NM 88310



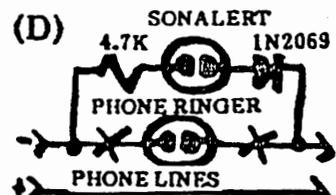
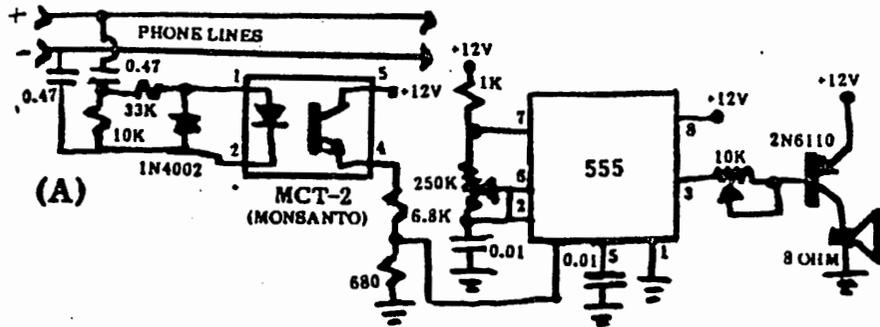
HOLD/MUSIC-ON-HOLD: This circuit uses a music synthesizer module (available in several tunes), sound-generating chip output, cassette or other audio input to provide music or special-effect sounds to those you have on hold. If you want the Hold function only, the transformer can be replaced with a 1.5K resistor. Or you can use a selector switch to select either Hold or Music-On-Hold. R1 should match the SCR used.



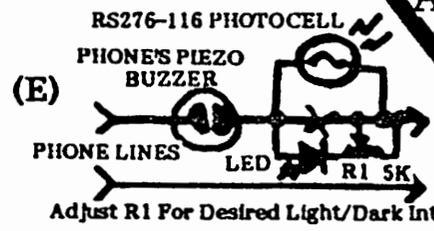
PHONE SPEAKER CIRCUIT: If you just want to listen, this circuit will let you do just that.



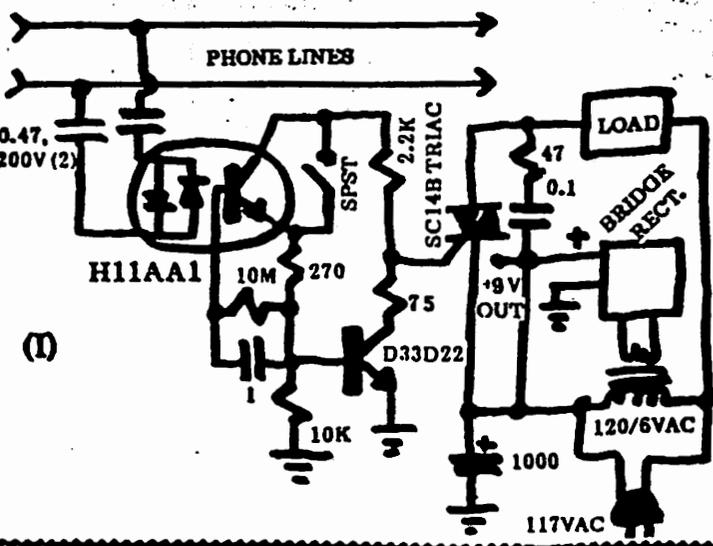
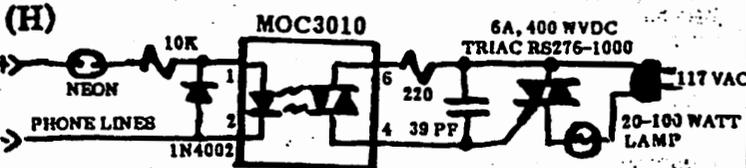
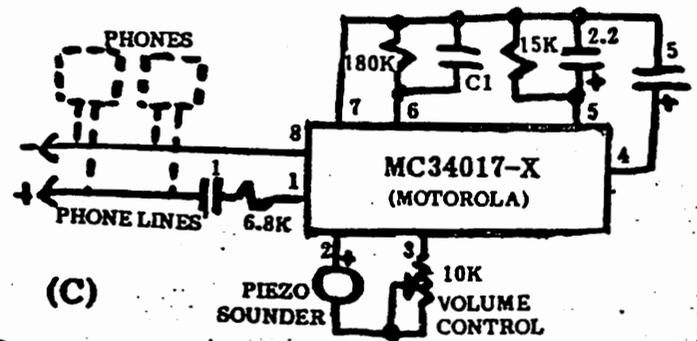
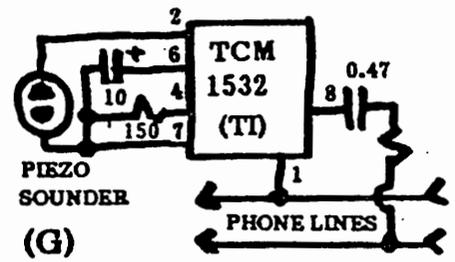
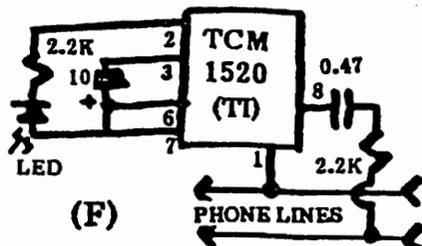
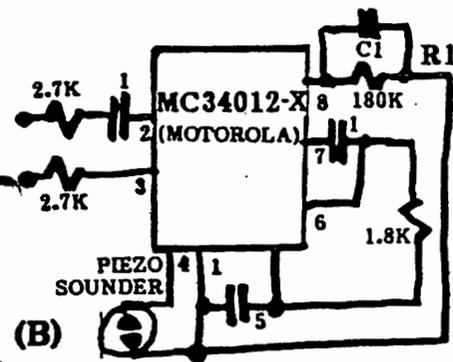
MISSSED CALL INDICATOR: If you are expecting a call, but can't be there to get it, this simple circuit will tell you that at least someone tried to call you. No hardwired connection is made to the phone circuit. You simply tape/glue the magnetic reed switch to the phone's bell coil. When a call arrives, it momentarily closes the switch, which activates the SCR and turns the lamp ON. Can also be used to activate a recorder or answering service.



PHONE
COLOR
BOX
ADDE
DUM



Adjust R1 For Desired Light/Dark Intensities



REMOTE RINGERS

The following are circuits that can be used to replace/supplement bell or piezo sounder now used as your phone's ringer. Most phone ringers can be completely turned OFF thru a built-in volume control. Else, disconnect the current ringer to replace it.

(A) This plain vanilla remote ringer uses an optical coupler for isolation, and a 555 to produce the desired ringer tone. A 555 (or 555s) can be used so that one 555 section is used to increase/decrease the ring time of the other 555 section, or to produce dual tone.

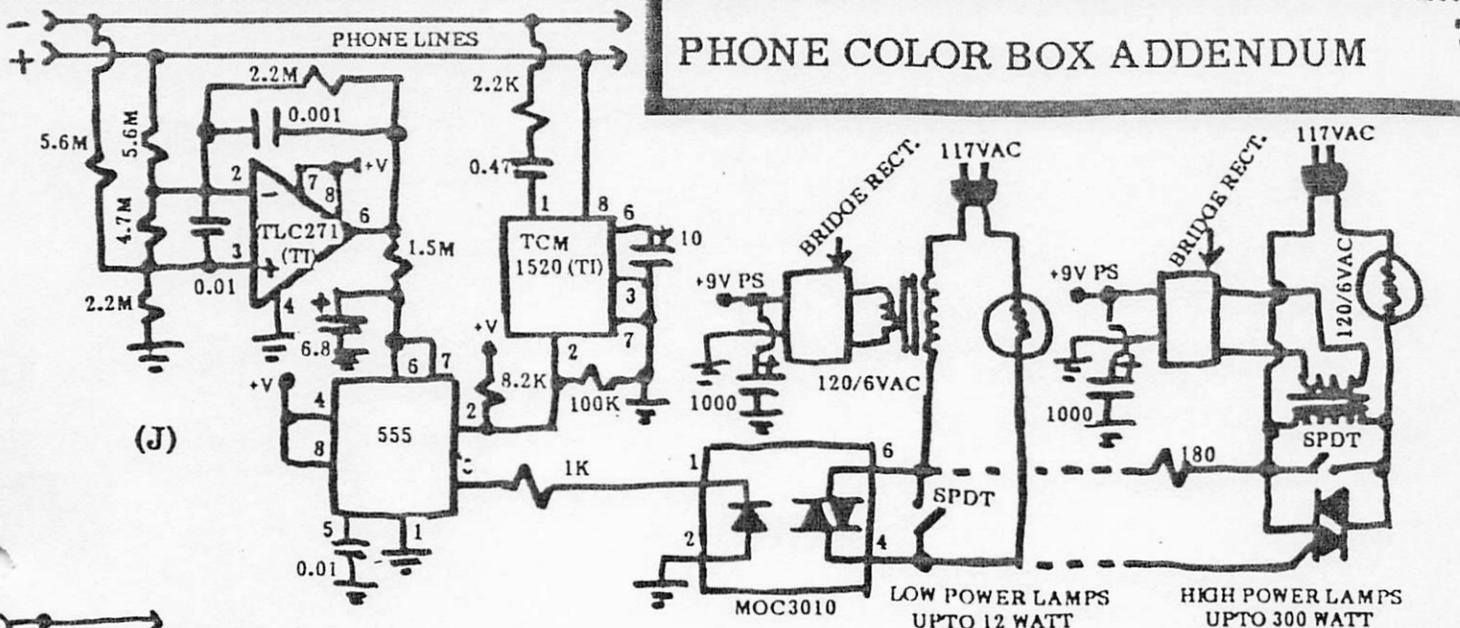
(B) This circuit produces a warble. There are three versions of MC34012 chip. The MC34012-1 warbles at 800-1000 Hz, the -2 at 16 2000 Hz, and the -3 at 400-500 Hz. C1 is, respectively, 1000 PF, 500 and 2000 PF. Phone line polarity is not important because the chip a built-in bridge rectifier. It also features transient protection direct drive for piezo sounders, and does not require external power. You can vary R1 and C1 to produce the warble most pleasing to you you are a country bumpkin like me, you can produce a turkey call using a C1 of 100 PF and a R1 of 68K. Then, you can get your phone calls at the barn even when the frost is on the pumpkin.

(C) This circuit uses another, similar Motorola device, to provide external warbler ringer. The three versions of the MC34017 use same C1 values for the same freq. ranges. For more information the MC34012 and MC34017, ask Motorola (Phoenix, AZ) for Application Notes AN933 and AN937, and the May 1988 issue of MODE ELECTRONICS, which includes plans for a theremin ringer.

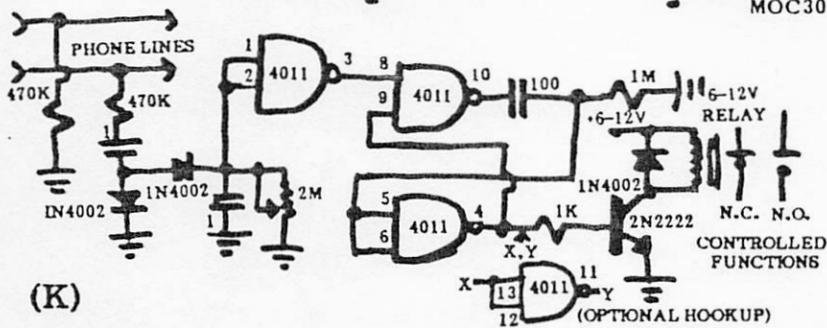
(D) This circuit is designed specifically for Mallory Sonalerts. Letting to the internal unit are clipped off and reconnected to replacement Mallory Sonalert:

- (1) SC-18, 3500 Hz, 70 DB, Soft.
- (2) SC-628, 2900 Hz, 80 DB, Medium.
- (3) SC-616N, 2900 Hz, 95 DB, Loud.

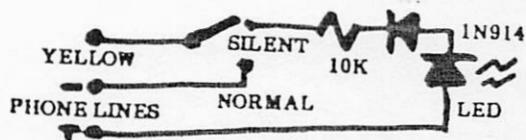
(E) This circuit automatically cuts OFF the phone ringer during night. A photo cell is wired in series with the ringer. When light the photocell, it conducts, and the ringer can ring. When darkened doesn't conduct and the ringer can't ring, instead an LED is used indicate ringing. To install, a lead to the ringer is cut and the photo (with 8" leads) is wired to both sides of the cut lead. A 1/2" hole carefully drilled into the phone's upper case half, and the photocell inserted and glued into place using silicon rubber cement. The phone placed under your night reading lamp or near a lighted window skylight.



(J)



(K)



(L)

CONSUMERTRONICS
2011 Crescent Dr., P.O. Drawer 537
Alamogordo, NM 88310

(F) This simple circuit is used to replace/supplement the phone ringer with an LED.

(G) This circuit is similar to (F) except that the new ringer is a piezo sounder. For combined results, combine both circuits in the same box.

(H) This simple circuit uses an opto-isolator and a triac to deliver the ring to a 20-100 watt lamp or other load. Ring detectors of this type are applicable to phone-controlled animal feeders, security checkers, etc.

(I) This circuit is a more complex but more refinable version of (H).

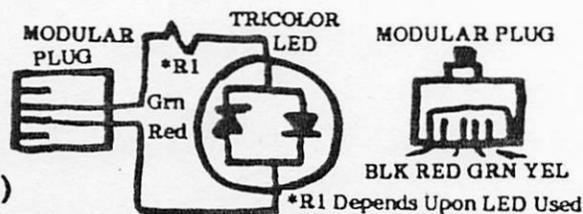
(J) This is the el deluxo version of (I). Can be used to control low-power and high-power loads. As long as the phone keeps ringing or the receiver is off-hook, the light will light steadily. It also remains lit a few seconds after ringing stops or you hang-up. It's ideal as a phone-controlled nightlight, and as a remote phone controller.

(K) This is another simple ring-activated circuit that uses a CMOS and relay.

(L) This circuit is a simple ringer replacer that is wired inside the desk phone's body and installed similar to the photocell described above.

PHONE TESTERS

These circuits are used to test and repair phone circuits:



(A)

(A) This circuit uses a tricolor LED to test the phone line. It is shown with a modular plug. Alligator clips or hardwiring work just as well, and any of these three methods can be used to hook up any phone circuit. Plug it into any phone jack. If the LED lights green, the jack is wired correctly (ie: green lead positive); if red, the jack is wired in reverse (ie: red lead positive). If the LED does not light, it means that the phone jack is dead, a handset has been lifted, there is an activated infinity bug on the line, or something else has loaded the line down. In fact, this simple device is an ideal continuous monitor for both defective phone conditions and infinity bugs.

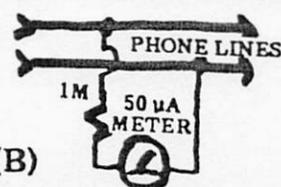
To test to see if your phone's off-hook functions, lift the handset. The light should extinguish.

To test for ring, dial your own phone number, then hangup just as the rings start. Your phone then should start ringing. If not, have a

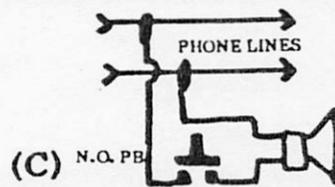
friend call you up. When your phone is ringing, the LED should pulse and be yellowish (due to AC component).

Conversation produces a varying, yellowish LED output.

A good source for modular plugs and other phone circuitry hardware is RADIO SHACK. We prefer MARLIN P. JONES & ASSOC., P.O. Box 12685, Lake Park, FL 33403 - they are often less than half price.



(B)



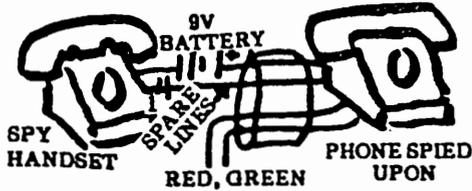
(C) N.O. PB

(B) This circuit uses a simple center-scale 50 uA (analog - not digital) meter to monitor the phone line. On-hook will show a high reading, off-hook a low reading, ring a pulsing reading, and conversation a varying reading. Can be used just like the LED tester, and, in fact, we suggest wiring both testers together.

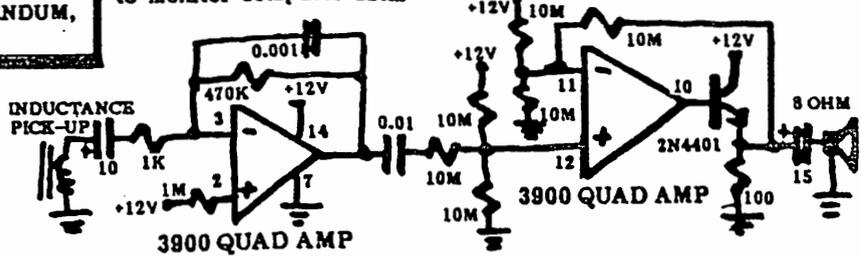
(C) This circuit uses an ordinary 8 ohm tweeter speaker and a push-button switch to test for dial tone. When the switch is pushed the speaker's low impedance loads the line to simulate the off-hook condition, and dial tone results. The PB function can be automated using a 555 chip and relay to periodically test the line, say during storms when the phone lines are down and you need help but you can't pick up the phone every minute to determine if the lines are fixed.

SECURITY

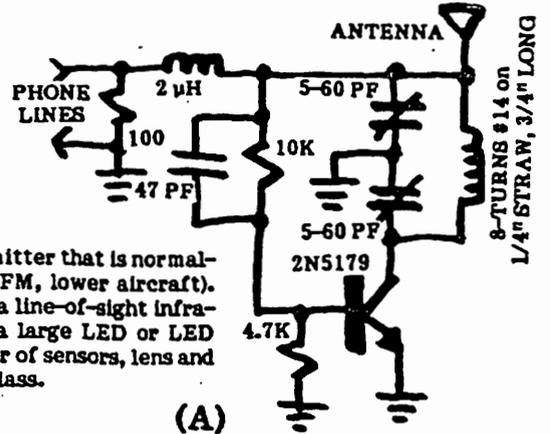
These nifty phone circuits are used for surveillance and eavesdropping purposes, and their countermeasures. For much more info. and circuits on phone bugging/tapping, see our TELEPHONE RECORDER INTERFACE (\$8) and SECRET & SURVIVAL RADIO (\$20) manuals. For much more info. on computer surveillance, see our COMPUTER PHREAKING, AUTOMATIC TELLER MACHINE, ATM ADDENDUM, and BEYOND VAN ECK PHREAKING manuals (\$20 each).



INDUCTANCE PICK-UP: This simple surveillance device is used with an inductance pick-up coil to monitor phone conversations and data. The coil can be a Lafayette 99E10340 pick-up coil, or it can consist of about 200 turns of fine enamel wire around an iron core. An old relay coil of about that size also works well. It is placed near the phone receiver for best results. The first 3900 stage is a high gain amp. The second stage is a unity-gain buffer amp, which output can also be used to monitor computer data.



SIMPLE PHONE EAVESDROPPER: Most phones use only two of the four lines going to it (Green and Red). In this circuit, the spare Black and Yellow lines are jumpered across the phone's speaker lines, with a 9V battery and 10 μ F capacitor in series, and wired to the speaker on a remote handset. The circuit will work without the battery and capacitor, but the extra loading may cause suspicions. See also the NE5900 circuit described herein. A variation of this technique is to connect the speaker of a speakerphone to a spare pair, and then wire it at the monitoring end to a low-impedance mike preamp, recorder, etc.

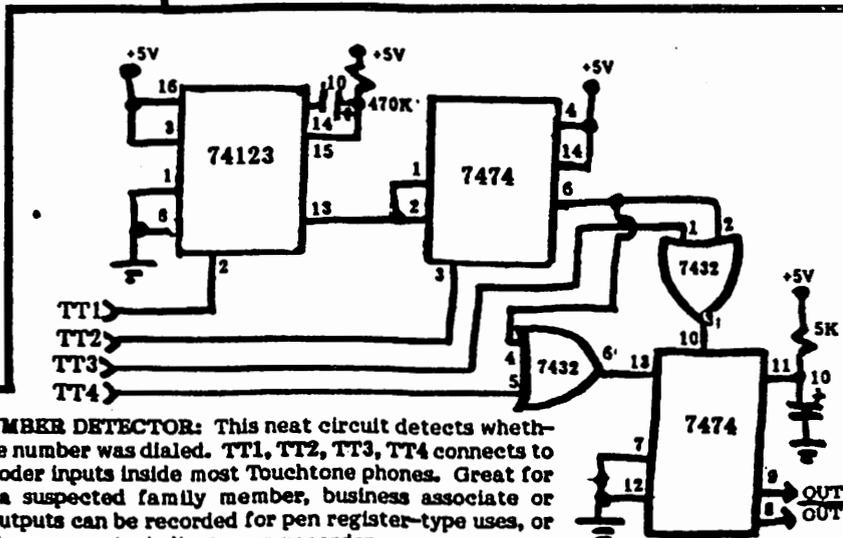
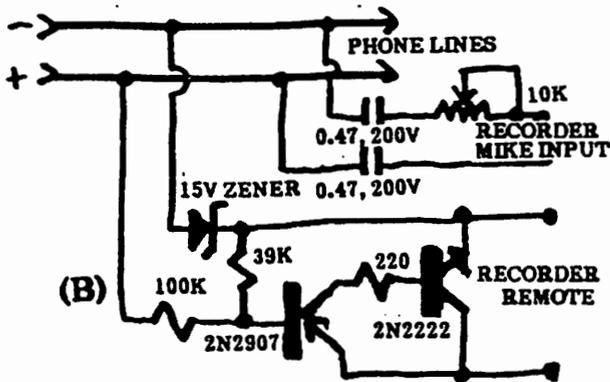
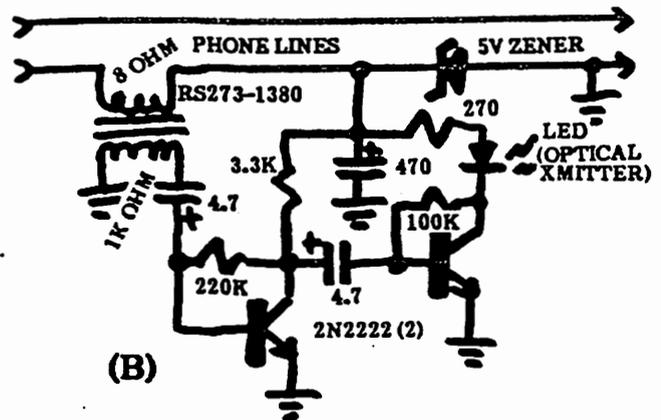
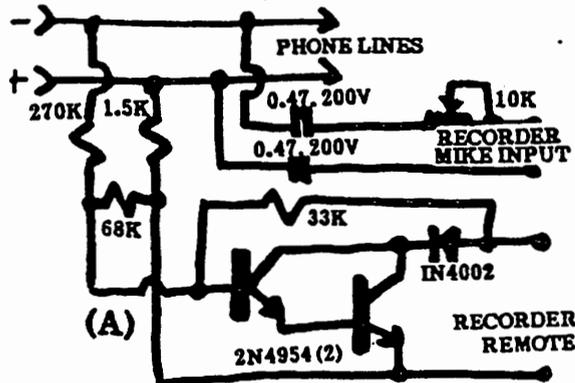


CONSUMERTRONICS
2011 Crescent Dr., P.O. Drawer 537
Alamogordo, NM 88310

BUGS/TRANSMITTERS: (A) is a radio bug/transmitter that is normally tuned between 108 MHz and 110 MHz (upper FM, lower aircraft). Use with care and don't violate FCC rules. (B) is a line-of-sight infrared bug/transmitter. For maximum range, use a large LED or LED cluster and a lens for the transmitter; and a cluster of sensors, lens and IR filter for the receiver. Will transmit thru glass.

SOLD FOR EDUCATIONAL PURPOSES ONLY

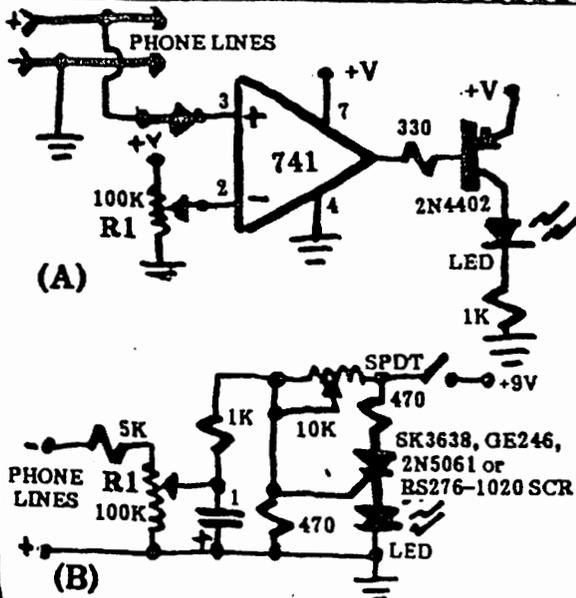
PHONE RECORDER SURVEILLANCE: (A) and (B) are fairly equal to each other and the \$29 Archer (Radio Shack) TELEPHONE RECORDING CONTROL. They are adequate, but detectable and destroyable phone recorder interfaces.



8

TOUCHTONE NUMBER DETECTOR: This neat circuit detects whether a certain phone number was dialed. TT1, TT2, TT3, TT4 connects to the sequence decoder inputs inside most Touchtone phones. Great for checking up on a suspected family member, business associate or employee! The outputs can be recorded for pen register-type uses, or to activate an alarm, remote indicator or recorder.

PHONE COLOR BOX ADDENDUM



BUG/EXTENSION DETECTORS: (A) uses a 741 as a comparator, while (B) uses the trigger circuit of an SCR for signal change detection. Another difference is that (A) activates only while the bug/extension is connected, while (B) can be made to stay ON even if the bug/extension is later disconnected (it also serves as a missed-call indicator). Bugs (some) and extensions tend to load the line. When they do, the properly set detector will immediately detect this loading and activate. Either can be used to detect on-hook or off-hook loading. To set (A)'s cut-off, adjust R1 to just cut-off the LED. To set (B), set R1 all the way positive, then adjust R2 to turn the LED ON. Then adjust R1 more negative to turn the LED OFF.

SMART USE OF AUTO REDIAL: A neat trick is to use the Auto Redial feature on most modern phones. Simply by pressing the Redial button, you can discover who was called last. If your home or business is burglarized, if the criminal made a phone call while there, his ID can be revealed. This happens often because criminals use a victim's phone to call friends, accomplices, fences, or to make free long distance calls. (All long distance calls and those local calls made on a line with measured service are also competely traceable from the phone bill.) Simply hook up a tape recorder with a Radio Shack or phone recorder circuit shown here or in our TELEPHONE RECORDER INTERFACE manual, turn the recorder ON, hit Redial and record the tones or rotary sweeps used in the last phone call (as well as the conversation you have with the called party). The number dialed can then be easily reconstructed. Or ask the police to do that for you.

Continued from P. 2

ORANGE BOXES

One color box that has gotten a lot of attention is the Orange Box (also known as the Killer Box). There have been many rumors about its existence. We long ago lost count of the number of promises from phreakers about Orange Boxes. One more promise and I'll scream louder than a nudist in a velcro jock strap!! We have yet to see one or verify that even one exists. Not even plans!

It is well known that, in New Jersey, Ma Bell tested a feature of Call Waiting that displays the calling number so that the subscriber can determine whether he should discontinue his current call to answer the waiting call. This feature resulted in outrage and legal challenges from the ACLU, unlisted subscribers, and others who love privacy.

It is known that this ANI (Automatic Number Identification) feature is NOT available anywhere without first subscribing to the Call Waiting service, and it is NOT available everywhere that Call Waiting is available. The implication is that only after subscribing to Call Waiting is the Ma Bell computer enabled for this ANI feature. We know from experience that no set of tones or digital signals sent down the line, either during ring or on-line conditions, produces a response from the Ma Bell computer that can be interpreted as a phone number. Enough said!

If you have an actual, proven Orange Box or the plans to one, or of an actual, proven REMOBS number, send it to us insured or certified (we don't accept unknown CODs). Otherwise, don't waste both of our time with bulls**t promises and fairy tales!

Illegal calling detected

Mountain Bell today announced that it has detected massive fraudulent use of interstate long distance calling that is causing disruption of telephone service in the Alamogordo area.

Area Manager Gene Whitehead said the sporadic disruption in service the past few days has been caused by the use of the Alamogordo switching facilities by people on the east coast calling Puerto Rico.

He said the use of the switching facilities became so in-

tense Wednesday that local subscribers were having to make many attempts to complete their long distance calls. Some subscribers could not make any long distance calls at all.

Whitehead noted that long distance calls into the area also were being blocked by the east coast traffic that was being routed to Puerto Rico illegally through the Alamogordo switch.

He said that the use of remote switching offices, such as the one in Alamogordo, to complete these types of long distance calls also causes disruption of local service.

For example, he explained, local telephone numbers are dialed as part of the total dialing sequence to complete such calls and this causes local telephones to ring. But when the telephones are answered, there is no one on the line.

Whitehead said every effort is being made to minimize the impact on local subscribers through electronic means, as the investigation continues in an attempt to remove the problem.

He said that this particular problem occurred in Alamogordo two years ago, and has appeared in other areas of the country. He said the perpetrators were using switching facilities in Montana, but were blocked there; they then tied into the Alamogordo exchange.

Other communities affected include Carrizozo, Tularosa and Cloudcroft.

Friday, October 31, 1986
Alamogordo, New Mexico

Phone companies fight fraud

Students, professionals and convicts cost firms hundreds of millions

WASHINGTON (AP) — Telephone companies are using computers, amnesty programs and the law to recoup their losses from a half billion dollars in unpaid calls a year.

College students, computer-literate professionals and even enterprising prisoners are among the offenders who get into the phone network illegally with stolen authorization codes, electronic devices or other means.

"Every time you find an answer for one area, another problem crops up. It's a continual battle," said Neal Norman, district security manager for American Telephone & Telegraph Co.

Companies are changing the software as well as the hardware in their networks to try to

block the calls, and they are offering amnesty programs on college campuses for students to "fess up and pay up."

They also are working with federal authorities to prosecute call-sell operators who are using stolen authorization codes and electronic "blue boxes" to break into the network and sell calls to all parts of the world at drastically discounted prices.

"The whole telecommunications industry is very aggressively pursuing the people who are committing fraud. They're going for restitution and jail sentences," said Rami Abuhamdeh, executive director of the industry-sponsored Communications Fraud Control Association.

Abuhamdeh estimated that the industry loses about 1

percent, or about \$500 million, to fraud annually, but he said, "It's tough to assess losses because it's a touchy topic with companies."

College students are believed to be among the biggest offenders. Many know how to use computers to search phone company systems for active authorization codes, and their campuses are hotbeds for large-scale theft because the codes are passed around so easily.

Other computer hackers include doctors, lawyers and homemakers, but Abuhamdeh said the heaviest damage is in selling the codes or posting them on "electronic billboards." The hackers themselves usually don't make as many calls as other groups, including prisoners, he said.

REMOBS

REMOBS (REMOte OBServation) is apparently another phreaker myth. Carriers are reported to have secret phone numbers that the phreaker dials using a Touchtone phone. He then punches in two access codes and the phone number he wishes to tap, which can be anywhere in the U.S. No operator comes on line. The tapping is done immediately, automatically, quietly (no telltale clicks, hums or beeps), and as long as he wishes.

Again, we have been promised REMOBS numbers without a single one ever being produced that can be shown to work. Neither we nor 2600 MAGAZINE (Spring 1988 issue, P. 27) believe that they exist (at least to the claimed power and extent). It's probable that each exchange has a REMOBS set-up for Ma Bell for line test purposes, and for law enforcement and other personnel for numbers in that exchange. And it's probable that once all the phone systems become completely integrated, a nationally-based REMOBS will be installed.

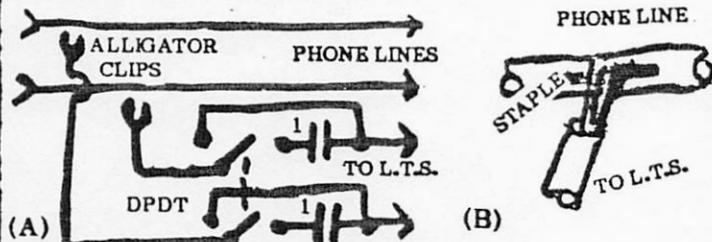
Phreakers have accessed certain Ma Bell functions in their exchanges by dialing DA (Directory Assistance) using a Silver Box. The "D" button is then held down. This bypasses the DA operator. A pulsed dial tone results. Access codes and phone numbers are then punched in the Touchtone pad. One of these test functions allows a quality check of a subscriber's line during actual use - thus eavesdropping.

The only known REMOBS-like system is the Teledyne Fortell System. It's limited to its exchange, and it requires passwords to access its various test functions.

LINEMAN'S TEST SET

The Lineman's Test Set (LTS), also known as the "butt set," can be bought commercially for \$100+. For a lot less, you can make one from a modified one-piece phone:

- (1) Use a line cord terminated with alligator clips. See (A).
- (2) Install a DPDT toggle switch and capacitors. See (A). When switched in, the capacitors block the line's DC, but permit the ring and conversation AC to be monitored.
- (3) Another hook-up method is to staple-connect bare ends of LTS leads to the phone lines. See (B). Another method is to poke the phone lines with small safety pins, then hook the alligator clips to them. Another method is to use a ribbon cable press-on connector. Then wire the LTS to the mating connector. Used where discovery is not likely, more than one phone line is monitored, and where the lines are repeatedly accessed over time.
- (4) The safest known way to use an LTS to phreak phone calls is to find a junction box serving public payphones and a cordless phone modified for LTS use. Even if the LTS is discovered, since the phreaker can be hundreds of yards away, he would be difficult to catch and convict.



MISCELLANEOUS

MORE ON COMPUTER BOX EMULATIONS:

Computers can be interfaced to phone lines to emulate color boxes in several ways. One method entails using a modem that can be programmed to generate multi-tones. Another is to couple your computer to the phone line using a speaker. This only works directly with computers that can generate multi-tones, such as the Amiga. IBM-PC/XT/AT and PS/2 systems can't generate multi-tones without the use of a special card. Else, a D/A conversion must be made that will produce these tones. A third, more practical way is to use a music synthesizer or MIDI to perform this task.

RIPPING-OFF PAYPHONES Cont'd:

Additional methods (P. 15-16) used to rip-off payphones include:
 (1) Using double-stick tape, Elmer's Glue or STP to gum-up coins.
 (2) Seal all leaks in the phone (money changer, ATM, etc.) with putty on a very cold, dark night. Fill the phone with water thru the coin slots. When the water freezes and expands, the phone bursts open.

A B C D DUAL-TONES:

The Touch-Tone table on P. 9 should be added to for the military (Auto-vo) phone system A, B, C and D keys. A = 697 + 1633. B = 770 + 1633. C = 852 + 1633. D = 941 + 1633. The result is a Silver or Grey Box. These extra keys are used to program in call priority.

SHRIEK MODULE:

CONSUMERTRONICS invented and sells a device called the SHRIEK MODULE (see our TELEPHONE RECORDER INTERFACE (\$8) manual for complete description). It works by sending an extremely loud shriek down the phone line at the push of a button. The SHRIEK MODULE is an excellent countermeasure against phone buggers, rapists, perverts, harassers, bill collectors, enemies, etc. It's quickly connected/disconnected with its modular phone plug and "Y" connector, both supplied with it. Our testing proves that the SHRIEK MODULE is easily loud enough to damage hearing. Some have scoffed at that claim, stating that it is impossible to build any device that can produce a loud enough sound over the phone to damage hearing. To settle this issue once and for all, below is part of an article photocopied from the ELECTRONICS DESIGNER'S CASEBOOK NUMBER 4, P. 5 (published by ELECTRONICS; emphasis is mine):

Acoustic protector damps telephone-line transients

by Gil Marosi
 Intech Function Modules Inc., Santa Clara, Calif.

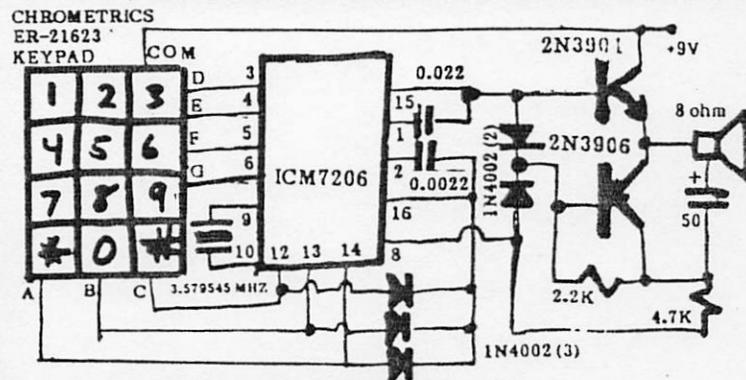
By limiting the transients on telephone lines, this acoustic shock protector prevents those sudden high sound levels that can damage the ear badly enough to cause loss of hearing. It holds the maximum peak-to-peak voltage at the receiver of a telephone headset to 50 millivolts.

Enough said! The SHRIEK MODULE sells for \$75 each (20% OFF on orders of 5-9 units).

MOBILE & CORDLESS PHONES:

The old style mobile phones were limited in range and number of channels. The user dialed the operator on a free channel and placed the call. The new mobile phones are called, "cellular" phones. They have many more channels and unlimited range because repeaters relay calls all over the U.S. and some parts of Canada, and no operator assistance is required. Cellular phones operate in the 870-890 MHz bandwidth, with channels spaced 30 KHz apart (from: SECRET & SURVIVAL RADIO (\$20)).

Cordless phones are mobile phones with a range of about 300 meters (a better antenna and receiver extends this range for miles). Older cordless phones could be accessed by anyone using their own cordless hand-



ANOTHER TOUCHTONE ENCODER: This one's similar to the previous one, except simpler to build. It's freqs. are strictly Touchtone.

VITAL INGREDIENTS

SWITCHING CENTERS AND OPERATORS

PHONE COLOR BOX ADDENDUM

Every switching office in North America (the NPA system) is assigned an office name and class. There are five classes of offices numbered 1 through 5. Your CO is most likely a class 3 or end office. All long-distance (Toll) calls are switched by a toll office which can be a class 4, 3, 2, or 1 office. There is also a 4X office called an intermediate point. The 4X office is a digital one that can have an unattended exchange attached to it (known as a Remote Switching Unit - RSU).

The following chart will list the office number, name, and how many of those offices existed in North America in 1981.

Class	Name	Abb.	# Existing
1	Regional Center	RC	12
2	Sectional Center	SC	67
3	Primary Center	PC	230
4	Toll Center	TC	1,300
4X	Toll Point	TP	
4X	Intermediate Point	IP	
5	End Office	EO	19,000
R	RSU	RSU	

When connecting a call from one party to another, the switching equipment usually tries to find the shortest route between the Class 3 end office of the caller and the Class 5 end office of the called party. If no inter-office trunks exist between the two parties, it will then move up to the next highest office for servicing (Class 4). If the Class 4 office can't handle the call by sending it to another Class 4 or 5 office, it will go to the next office in the hierarchy (3). The switching equipment first uses the high-usage interoffice trunk groups. If they are busy it goes to the final trunk groups on the next highest level. If the call cannot be connected then, you will probably get a reorder [120 IPM (Interruptions Per Minute) signal also known as a fast busy]. At this time, the guys at Network Operations are probably going berserk trying to avoid the dreaded Network Deadlock (as seen on TV!).

It is also interesting to note that 9 connections in tandem is called ring-around-the-rosy and it has never occurred in telephone history. This would cause an endless loop connection (an interesting way to really screw up the Network).

The 10 regional centers in the United States and the 2 in Canada are all interconnected. They form the foundation of the entire telephone network. Since there are only 12 of them, they are listed below:

Class 1 Regional Office Location	NPA
Dallas 4 ESS	214
Wayne, PA	215
Denver 4T	303
Regina No. 2 SPI-4W [Canada]	306
St. Louis 4T	314
Rockdale, GA	404
Pittsburgh 4E	412
Montreal No. 1 4AETS [Canada]	504
Norwich, NY	607
San Bernardino, CA	714
Norway, IL	815
White Plains 4T, NY	914

In the Network, there are three major types of switching equipment. They are known as: Step, Crossbar, and ESS. Check past and future issues of 2600 for complete details on how these systems work.

Operators
Another vital ingredient of the Network is the telephone operator. There are many different kinds. What follows is a discussion of some of the more common ones.

TSPS Operator. The TSPS [Traffic Service Position System (as opposed to This Shitty Phone Service)] Operator is probably the bitch (or bastard for the phreak liberationists) that most of us are used to having to deal with.

Here are her responsibilities:
1) Obtaining billing information for Calling Card or 3rd number call.

- 2) Identifying called customer on person-to-person calls.
- 3) Obtaining acceptance of charges on collect calls.
- 4) Identifying calling numbers. This only happens when the calling number is not automatically recorded by CAMA (Centralized Automatic Message Accounting) and forwarded from the local office. This could be caused by equipment failures (ANIF - Automatic Number Identification Failure) or if the office is not equipped for CAMA (ONI - Operator Number Identification).

(I once had an equipment failure happen to me and the TSPS

operator came on and said, "What number are you calling from?" Out of curiosity, I gave her the number to my CO, she thanked me, and then I was connected to a conversation that appeared to be between a frameman and his wife. Then it started ringing the party I originally wanted to call and everyone phreaked out (excuse the pun) I immediately dropped this dual line conference!

You shouldn't mess with the TSPS operator since she knows where you are calling from. Your number will show up on a 10-digit LED read-out (ANI board). She also knows whether or not you are at a fortress tone and she can trace calls quite readily. Out of all of the operators, she is one of the most dangerous!

INWARD Operator. This operator assists your local ISPS ("0") operator in connecting calls. She will never question a call as long as the call is within her service area. She can only be reached via other operators or by a Blue Box. From a BH, you would dial KP*NPA*121*ST for the INWARD operator that will help you connect any calls within that NPA only.

DIRECTORY ASSISTANCE Operator. This is the operator that you are connected to when you dial 411 or NPA-555-1212. She does not really know where you are calling from. She does not have access to unlisted numbers, but she does know if an unlisted number exists for a certain listing.

There is also a directory assistance for deal people who use Teletypewriters (TTY's). If your modem can transfer BAUD01 (45.5 baud - the Apple Cat can), then you can call him/her up and have an interesting conversation. The number is 800-855-1155. They use the standard Telex abbreviations such as GA for Go Ahead. They tend to be busy and will talk longer than your regular operators. Also, they are more likely to be persuaded to give more information through the process of "social engineering."

Unfortunately, they don't have access to much. I once bullshitted with one of these operators and I found out that there are two such DA offices that handle TTY. One is in Philadelphia and the other is in California. They have approximately seven operators each. Most of the TTY operators seem to think their job is boring. They also feel they are underpaid. They actually call up a regular DA # to process your request - no fancy computers here! (Other operators have access to their own DA by dialing KP*NPA*131*ST (MF).

The TTY directory assistance, by the way, is still a free call, unlike normal DA. One might be able to avoid being charged for DA calls by using a computer and modem at 45.5 baud.

CN/A Operator. CN/A operators do exactly the opposite of what directory assistance operators are for. You give them the number, they give you the name and address (Customer Name; Address). In my experiences, these operators know more than the DA operators do and they are more susceptible to "social engineering." It is possible to bullshit a CN/A operator for the NON-PUB DA# (i.e., you give them the name and they give you the unlisted number). This is due to the fact that they assume you are a fellow company employee. The divestiture, though, has resulted in the break-up of a few NON-PUB #'s and policy changes in CN/A.

INTERCEPT Operator. The intercept operator is the one that you are connected to when there are not enough recordings available or the area is not set up to tell you that the number has been disconnected or changed. They usually say, "What number did you dial?" This is considered to be the lowest operator lifeform since they have no power whatsoever and usually know very little.

OTHER Operators. And then there are the: Mobile, Ship-to-Shore, Conference, Marine, Verily, "Leave Word and Call Back," Route and Rate (KP*800*141*1212*ST - new number as a result of the break-up), and other special operators who have one purpose or another in the Network.

Problems with an Operator? Ask to speak to their supervisor...or better yet, the Group Chief (who is the highest ranking official in any office), the equivalent of the Madame in a whorehouse (if you will excuse the analogy).

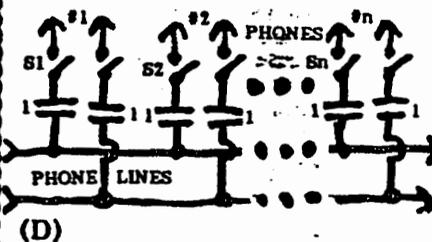
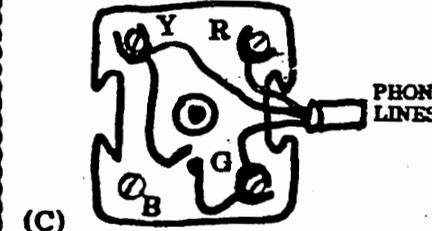
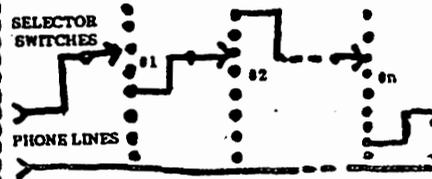
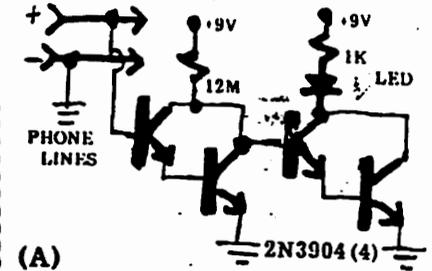
Some CO's, by the way, have bugs in them that allow you to use a 1 or a 0 as the 4th digit when dialing (This tends to happen mostly in crossbars and it doesn't work consistently.) This enables a caller to call special operators and other internal teko numbers without having to use a blue box. For example, 415-121-1111 would get you a San Francisco-Oakland INWARD Operator.

From: 2600 MAGAZINE
P.O. BOX 752, MIDDLE ISLAND, NY 11953

SUBSCRIPTIONS: \$15/yr Individuals,
\$40/yr Corporations

BACK ISSUES: \$25/yr, since 1984

2600 is a highly recommended phone and computer phreaking quarterly



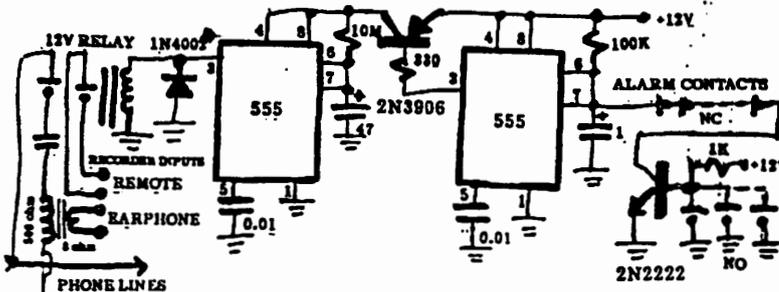
SIMPLE PHONE CIRCUITS: (A) is another Off-Hook indicator. Circuit isolation and input impedance are very high. (B) is a phone lock. Once you have the circuit wired, then seal your box with epoxy to conceal the combination. Prevents unauthorized people from using your phones. Any number or type of selector switches can be used. (C) is a simple ringer silencer that does not require disassembly of the phone. The line connecting the yellow and green leads is cut and the cut ends wired to a SPST switch. (D) is a simple conference caller. To use this circuit, each phone shown must have its own number. Use one phone to call Person A, and another phone to call Person B. Then throw the switch that connects the two phones together thru their 1 µF caps. Bingo! You're in conference!

set, at the cost of the subscriber. Newer models use different freqs. and access codes to prevent this lucrative form of phreaking. Channel 1-10 Base and Handset freqs. (In MHz) are, respectively:
1 - 46.61/49.67 2 - 46.63/49.845 3 - 46.67/49.86
4 - 46.71/49.77 5 - 46.73/49.875 6 - 46.77/49.83
7 - 46.83/49.89 8 - 46.87/49.93 9 - 46.93/49.99
10 - 46.97/49.97

SUGGESTED READING:

The following selections are suggested:
(1) 2600 MAGAZINE - an excellent quarterly on phone and computer phreaking. P.O. Box 752, Middle Island, NY 11953. Subscriptions are \$15/yr. individuals, \$40/yr. corporate. \$25/yr. back issues (since 1984). The Spring 1988 issue has a lengthy article called, "MONITORING PHONE CALLS WITH A TVRO." We reproduced this article in our new, BEYOND VAN ECK PHREACKING (\$20) manual.

PHONE COLOR BOX ADDENDUM



ALARM DIALER: This invaluable circuit will detect the activation of one to many normally-closed (NC) or normally-opened (NO) switches common to alarm systems, then automatically dial the phone using Touchtones, and then play a message into the phone. The number dialed can be 911 or some phone number you, or someone you trust, can be reached at. Alarms include those for intrusion, fire, smoke, water, ice, wind, pet, etc. Additional circuitry (using the NE5900 IC described herein) could be added to detect a busy signal or non-answer, and to dial a another number if either occurs.

To use this circuit, first record the tones used to dial the number. This can be done by using any phone recorder interface hooked up to your recorder while you dial that phone number. Leave 2-5 seconds of lead tape before dialing so that enough time is given for the dialtone to come on. Then leave 3-6 seconds of blank tape. Then follow that with a short, clear, emergency-type message that includes your name and address. Follow the message with another 3-6 seconds of blank tape. Repeat this message and 3-6 seconds of blank tape at least 10 times or until about 8.5 minutes of tape time is used up. Then rewind the tape, and hook the circuit to it. Once completed, test the device by simulating an alarm activation. Then rewind your tape again.

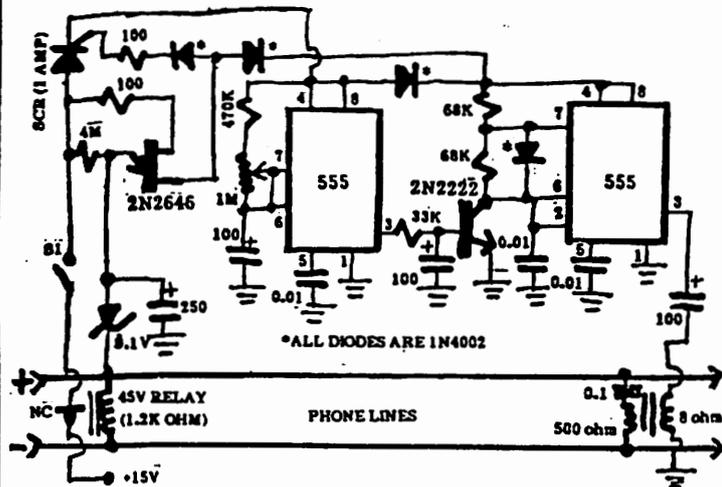
(2) "TELEPHONE ADD-ON, NO MORE WRONG NUMBERS," Gary McClellan, *RADIO ELECTRONICS*, March 1984, P. 59. This fairly complex device ends you the misery of wrong-number dialers, phone salesmen, harassers, etc.

(3) "THE BLUE BOX AND MA BELL," Herb Friedman, *RADIO ELECTRONICS*, P. 49. Fascinating article on early phone phreaking but does have some major errors (ex: misidentifying the Black Box as the Red Box).

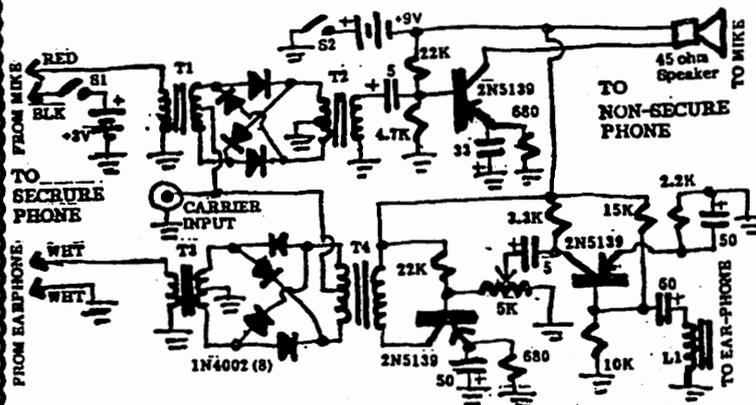
(4) PHREAKER BBS. Error rates are high, much of the material is pure fantasy and nonsense, the schematics are virtually unreadable and no photos, BBSs can be expensive to access, some use plagiarized material, and phreaker BBS deny most users important accesses and their numbers change so frequently that its hard to keep track of them. Occasionally you can pick up some useful info. We use BBSs but mostly to download PD software, for E-Mail, and for exchanging opinions.

"PHRACKING":

The correct term for describing color boxing is "Phreaking." The term, "Hacking," can be defined as using computers and the phone system to penetrate other computer/phone systems. "Phreaking" has also been defined this way. "Hacking" can also simply be defined as computer programming. It's time that a new term be devised which is defined as any kind of phreaking/hacking activity that involves a computer and the phone system. I propose that my new term, "PHRACKING" be used and relegate "Phreaking" to color boxing only and "Hacking" to programming only. The term, "PHRACKING" not only combines "Phreaking" and "Hacking," but also sounds like "Cracking," "Fragging" and "Fracas," all relevant terms. If you agree/disagree, please write me (please don't phone until science develops a way to clone about three more of me).



PHONE CALL LIMITER: This neat device limits the duration of a phone call. Great if you have talkative teenagers or employees. The amount of time permitted is about 10 minutes. After about 8 minutes (set by the UJT circuit), several warning beeps are emitted on the phone line. (This duration can be changed by changing the 4M ohm resistor and/or 250 μ F capacitor. Using a 1.2M ohm resistor keeps the calls under 3 minutes for long distance calls.) From about 1-3 minutes later (set by the 555, 470K, 1M and 100 μ F), a constant ringing across the line results that can only be stopped by hanging up the phone. This circuit is automatically activated every time the receiver is picked up and reset upon hanging up, but can be defeated by opening up S1.



SECURITY VOICE SCRAMBLER/DESCRAMBLER: This circuit lets you use an ordinary phone to scramble and transmit a voice message and receive a scrambled message and descramble it. It is a frequency inverter scrambler. This means that low tones are inverted to high tones and vice-versa. To an eavesdropper, the resulting message is garbled or like a foreign language. Each phone involved in a scrambled call must have one of these devices for it to properly work.

This circuit requires the mechanical construction of a receiver mount that allows the small pickup coil, L1, to be placed near the house phone's earphone, and a small speaker near its mike. This mount should also include the rest of the circuitry.

L1 is a telephone induction coil pick-up, such as the Lafayette 89E10340 or equivalent (iron coil form). Some relay coils also work well. T1-T4 are all 1:1 isolation transformers with 500 ohm windings, such as the Triad T34-X. 300-600 ohm windings will also work. The carrier input can be any sinewave generator tunable in the 3-3.05 KHz range. For any set-up all carrier freqs. used must be identical.

TELEPHONE RECORDER INTERFACE

COPYRIGHT © 1985, JOHN J. WILLIAMS & FAMILY. ALL RIGHTS RESERVED
By: John J. Williams, MSEE, CONSUMERTRONICS CO., P.O. Drawer 537, Alamogordo, NM 88310

How often have you needed to record a telephone conversation without the fear that Ma Bell or some goon can detect that you have a recorder hooked-up to your lines? Ultra-high impedance telephone interfaces, such as the TELECORDER (described here) were difficult to obtain by the unwashed general public. Ma Bell, police agencies, spy outfits and organized crime families had them. (Sidetone inductive taps have been available, but require the disassembly of the phone.)

A telephone recorder interface should have the following features:

(1) It must provide a clear and clean reproduction of the conversation.

(2) It must be quickly and easily connected and disconnected. With the advent of the modern phone connector, one no longer needs a screwdriver to make a phone connection.

(3) It must be easy to operate, and of small size.

(4) It must have ultra-high input impedance; it must not load the lines or interfere with telephone conversations; and it must not be electronically detectable. The old-fashion interface consisting of a capacitor(s) and a transformer (see figure) to connect a recorder to the phone lines is easily detectable. Sophisticated electronic techniques can be used to even ferret out taps/bugs with input impedances of up-to about 10 Meg. ohms. The lines are thoroughly tested when they are known to be clean, and then periodically retested for taps/bugs. Any changes in line impedances, which indicate a tap/bug, can then be observed. Even minute changes will alert the tester to make a physical search.

(5) It must be rugged and dependable. Regardless of the noise and interference on the lines, the recorder interface must survive and function as designed. It must also survive high-voltage tap/bug destruction techniques. To destroy bugs/taps, a technician disconnects the lines from all legitimate devices and the Central Office. He then hooks-up an AC generator to supply 1,000+ volts to the lines. Any tap or bug on the lines not of very high impedance and surge-protected as the TELECORDER is, is immediately destroyed.

(6) It must have on-line monitoring capabilities. In other words, simply by observing an LED or meter, one can tell if there is activity on the lines without lifting the handpiece. On-line monitoring is extremely important for two reasons. First, it immediately detects any tap/bug in which the monitored conversation is sent down the phone lines, such as an infinity bug. A tap/bug is obvious when, as in any recording, you notice the sound-level LED/meter activations are in sync. to the sound levels in the room. Second, it immediately detects when an extension phone is being used. In this case, the sound-level LED/meter activations will indicate a conversation is taking place, but since the sound activations are not in sync. with the room sounds, the sound is coming from an extension.

(7) A nice feature is an option to have the recorder activate from an off-hook or voice-activated switch. We implemented an electronic off-hook activation switch. When it comes to phone conversations, off-hook switching is preferred over voice-activated switching.

(8) Another nice feature is to have a "Shriek" option. The "Shriek" is designed to send an ear-piercing shriek down the phone lines to protest against dirtbags that make obscene or heavy-breathing phone calls, and against infinity bug eavesdroppers. We also implemented this feature.

TERMINOLOGY

The term "phone" means "telephone." The term "recorder" means "cassette tape recorder." The term "mike" means "microphone." The abbreviations, "RF" and "FM" mean "radio frequency" and "frequency modulated," respectively.

The term "phone tap" or "tap" is used for "telephone wiretap." A phone wiretap occurs when an electrical connection is made to the phone lines for the purpose of monitoring the signal on the lines. For example, if one uses alligator clips to jumper a headset across the phone lines, that is wiretapping. The TELECORDER is a form of wiretapping. Wiretaps are generally most easily placed without entering the premises to be tapped. Phone taps are used to monitor phone conversations only.

The term "phone bug" or "bug" means "telephone bug," and describes any device, other than a tap, which is installed in a phone or connected to one, and is used to monitor a conversation. Although the terms "tap" and "bug" are frequently and incorrectly used interchangeably when phone devices are described, a "bug" is generally a device that uses its own microphone and transmits wirelessly. However, a bug may be connected to the phone lines to obtain operating power, to provide switching, and/or to transmit on a wired basis. Telephone bugs are frequently placed to not only monitor phone conversations, but all conversations taking place in the room. A "bug" almost always requires entering the premises to be bugged. The objective of bugs and taps are the same - to compromise conversation.

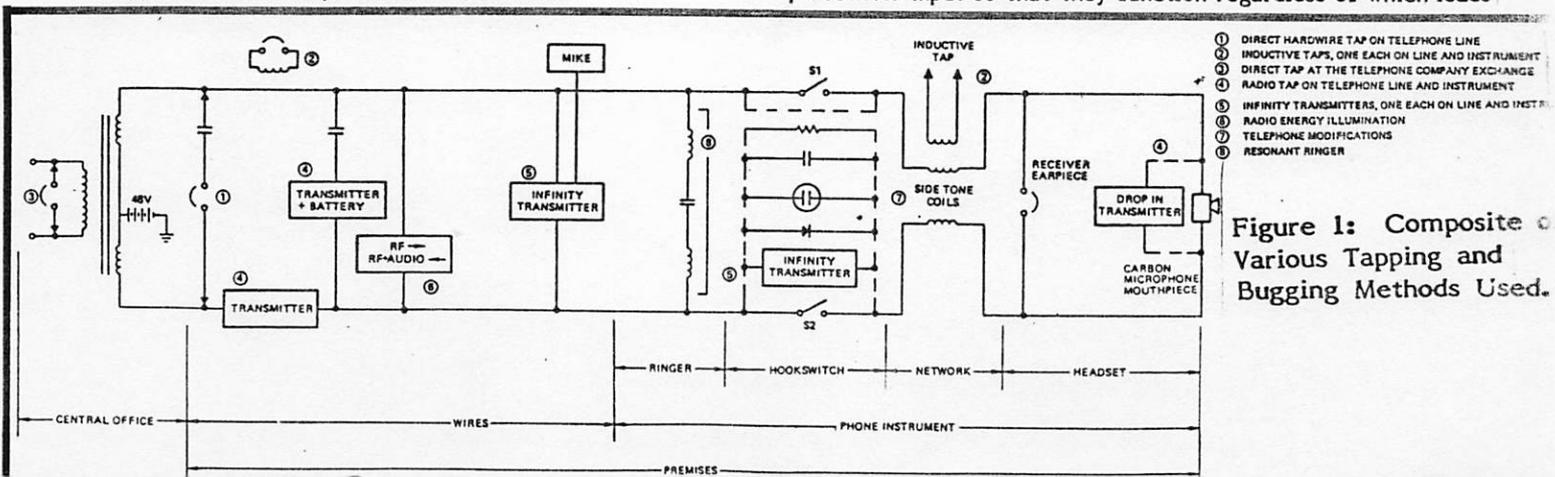
INFINITY BUG

One of the most popular phone bugs is known as the "infinity bug," "infinity transmitter" and "harmonica bug." This fascinating device is secreted inside the phone and connected directly to it for switching and transmitting purposes. It usually also derives its power from the phone lines. Once implanted inside the phone, the eavesdropper can call the phone from any place in the world. Before the phone rings, he uses a harmonica (or other tone signal device) to inject a certain frequency into the lines. The infinity bug detects this frequency and immediately switches off the ringer and then bypasses the hook-switch switches to make the phone act as if the handpiece had been lifted. The signal from the now active handpiece mike (or from another mike hidden in the phone or in the room) is highly amplified by the infinity bug and transmitted down the lines to the eavesdropper. The infinity bug immediately becomes deactivated when either the handpiece is physically raised or when the eavesdropper injects another turn-OFF tone into his phone.

HOW THE CIRCUITS WORK

The TELECORDER circuits shown here are (refer to figures): 1) The TELECORDER, Shriek Circuit, and Power Supply. 2) The Automatic (Auto.) Feature. 3) The add-on RF Transmitter Circuit.

Most commercial telephone recorder interfaces have a bridge rectifier input so that they function regardless of which leads



are connected to the red and green lines. We do not recommend bridge rectifier inputs because they are vulnerable to high voltage line-clearing pulse techniques. Therefore, proper connection is required for the TELECORDER to function. The red line should be positive with respect to the green line.

TELECORDER WITH SHRIEK CIRCUIT

The 2N43383 input pre-amp. is biased-up with R1 to permit an ultra-high input impedance. Optimum results occur when R1 is tuned so that $V_s = 0.65 \cdot V_{dd}$. The input zener protects the circuit from high voltage or reverse inputs. The output of the pre-amp. goes to the Aux. Input of the recorder. The input impedance of the Aux. Input of cassette recorders are typically 100 K - 500 K ohms. The Mike Input is not used because its input impedance is too low - typically 10 K ohms. To provide a stronger signal to the recorder, use the audio amplifier stages of the RF Transmitter (see figure) to boost the output of the FET. This output is then connected to the Mike Input of the recorder.

The Shriek Circuit simply consists of a NE555 Timer IC coupled to the phone lines with a standard 500:8 ohm miniature speaker transformer. The capacitors in series with its primary and secondary block the DC. When the ganged push-button switch is closed, two things happen - power is fed to the timer to activate it, and the transformer secondary is connected to the phone lines. The second feature is very important because, without it, the Shriek Circuit would have to be permanently connected to the phone lines, and thus would be detectable by Ma Bell and other snoopers. R2 is tuned so that the resultant output is as sharp as possible for optimum effectiveness.

The Power Supply Circuit is basically a plain vanilla design, except that an AC outlet for the recorder AC is provided. SW1 may/may not be included for switching the Auto. Feature into the circuit, and for independent recorder operation. We designed our power supply for 15 VDC (7815 voltage regulator IC), but you can select a different voltage. You can always use batteries if 120 VAC is not desired or available.

AUTOMATIC FEATURE

The Auto. Feature Circuit is an option that permits you to automatically turn-ON the recorder whenever the phone is in the off-hook state. Note that the Auto. Feature is NOT a voice-activated switch. With this option, even the dial pulses/tones are recorded, and infinity bugs automatically activate the recorder. The purpose of the Off-Hook Detection Circuit is to provide a +15 VDC at the collector of the 2N2222A transistor whenever the input voltage drops from the 48 volt on-hook phone line voltage to the 5 - 6 volt off-hook line voltage. The purpose of the Delay Circuit is keep the recorder ON for 1 - 25 seconds (determined by 1 M, 15-turn pot.) after the last off-hook situation. This saves wear and tear on the recorder so that it doesn't keep turning ON and OFF whenever the phone rings.

The 15 volt input zener is provided to protect the circuit from line noise and surges. Input impedance is an impressive 30 M ohms. The 5 volt source zener is used to drop the output voltage at the 2N2222A input for proper switching. It, as well as the 15 volt zener, must be changed if a power supply voltage other than 15 volts is used. SW1 on the CD4047 output selects either the Auto. Feature circuit to control the reed relay (this recorder), or to bypass the Auto. Feature altogether.

RF TRANSMITTER

In case you want to transmit the monitored phone conversations, an RF transmitter circuit is provided. The input is connected to point (A) on the TELECORDER FET source output. The first two stages amplify the input signal, and provide high stability and sensitivity. The last two stages mix the signal with the carrier and transmit it as a FM signal. Maximum practical range is about 10 miles. Any quality FM receiver will receive the signal.

CIRCUIT TESTING

The TELECORDER is not difficult to test. You do not need anyone to call you for the preliminary tests. You can dial yourself using your own phone. Dial your number. When ringing commences, hang-up. Your phone should ring as if you were called by someone else. The Central Office doesn't know the difference. By picking up the handpiece, you can talk to any phone extension. Because the TELECORDER is ultra-high input impedance, you can test and use it without any fear of being electronically detected by Ma Bell or anyone else.

Test the Shriek Circuit to the bare minimum. Just enough to tune it for optimum output.

Once testing is completed, you are ready to put your TELECORDER to work for you.

TIPS AND SUGGESTIONS

1) Depending upon how you wish to use the TELECORDER will dictate its size, shape, arrangement of controls, AC power vs. battery operation, and so forth. We used a 6" X 9" X 2" aluminum hobbyist box (see figure) so that we could place the recorder over it, and the phone on top of the recorder.

2) We purposely designed the TELECORDER to provide all the desired features with the greatest simplicity of design. Commonly available components were selected. Substitutions of equivalent devices can be made. Components should be readily available from Radio Shack, other retail electronic stores, and ads in the various electronics/computer magazines. Although we prefer to wire prototype circuits using point-to-point wiring on flea clips and perf. board because wiring changes are much more easily made, you might want to finalize your design on a PC board for greater compactness and less noise.

3) Component quality is important - particularly when it comes to noise figure. All input resistors should be metal oxide types - never carbon! Capacitors should be quality tantalum or mylar (except for the 1,500 uf electrolytic power supply filter capacitor). Either operate the TELECORDER from a battery, or provide at least 1,500 uf of filter capacitance. The best quality CMOS components are RCA.

4) Since the FET inputs are ultra-high impedance, be careful to keep great distance between input leads and AC power (either internal or external) and oscillator and output sections. Input leads should be of the shortest lengths possible. The input FETs should also be separately shielded within the circuit box, and liberally use ground planes. Use sound wiring techniques. All external signal leads should either be shielded (preferred) or twisted pair.

5) The choice of recorder and cassette tape are also critical. The Realistic (Radio Shack) CTR-40 recorder chosen was of a handy size, but did not impress us as high quality. Be sure that your recorder has an Aux. Input, a Remote Input, and either a sound-level LED or meter (preferred). Keep the tape heads cleaned. The cassette tape should be of the best quality you can buy.

6) By using sound wiring practices, and top quality electronic components, recorder and tape, and by keeping input leads away from stray AC sources, you can make excellent recordings. If not, noise level can be so high that the resultant quality is very poor. In fact, quality can become so poor that you may not be able to pick up soft voices. Remember that the signal has to be picked off of the usually noisy phone lines, and then processed by the TELECORDER circuitry, the recorder circuitry and tape heads.

PREVENT PHONE EAVESDROPPING

Although there are many ways to tap/bug a phone, there are only three methods of obtaining the purloined conversations: 1) Over the phone lines. 2) Using an RF transmitter/receiver. 3) A hard-wired recorder or headset.

To ferret out all taps and bugs on a regular basis is an expensive, time-consuming and uncertain proposition. Circuits using the type of ultra-high impedance input used by the TELECORDER and non-electrical taps (ex: inductive) can only be revealed by physical discovery. We feel that a better approach is to prevent the transmission of the stolen information. The steps described below will stop most phone leaks, but can be circumvented by Ma Bell, police agencies and top-of-the-line detectives:

1) Use the TELECORDER to monitor the lines so that you can immediately detect the presence of an active infinity bug or other tap/bug that uses the phone lines for transmission.

2) Place the telephone inside of a fine mesh hardware cloth booth securely grounded to a coldwater pipe. For cosmetic purposes, the booth can be surrounded by plastic, fiberglass or wood. This eliminates RF transmissions from bugs/taps located inside the phone. Other methods include locking the phone up in a safe when not in use, and epoxing the chassis screws and screw caps after thoroughly inspecting the phone's innards. A fifty dollar phone is a small price to pay to protect millions of dollars of information.

3) Rewire the phone so that it runs in visible metal conduit as far as you can, and frequently inspect these runs for physical invasions. Eliminate all extensions.

Consumertronics Co.

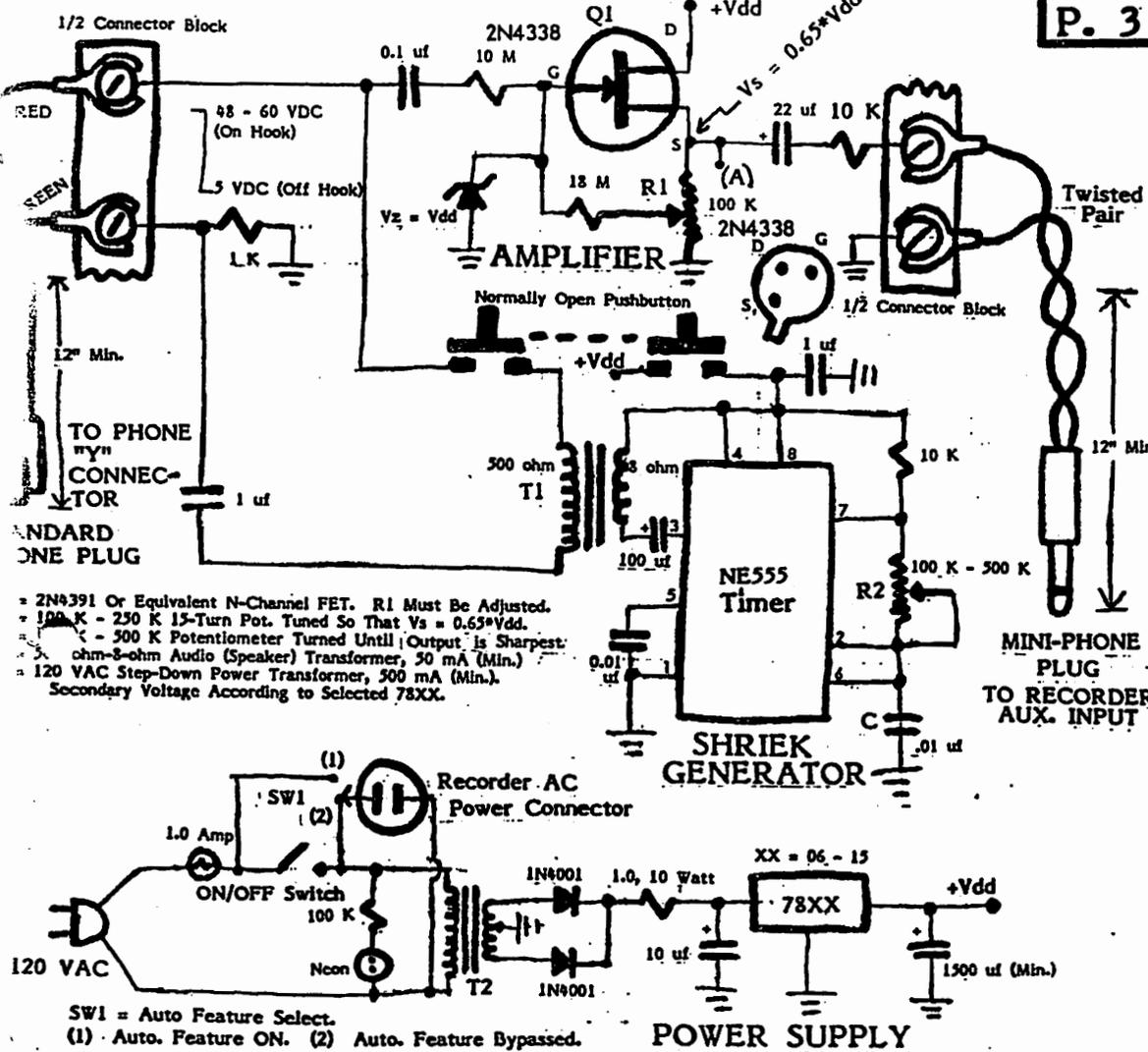
2011 CRESCENT DR., P. O. DRIVE 537,
ALAMOGORDO, NM 88310

Every reasonable attempt is made to provide complete and accurate information; CONSUMERTRONICS CO. is not liable for any errors or omissions found herein. If you find any errors or omissions, please write us. If substantial, or you provide us substantial new information we publish in the future, we will pay you cash and/or provide you a byline in the next edition. Sorry, we do not have sufficient staff to provide individual advice.

TELEPHONE RECORDER INTERFACE IS SOLD FOR EDUCATIONAL PURPOSES ONLY. The legality of using the TELERECORDER is questionable to the best of our layman's knowledge. As long as you use the TELERECORDER to record a phone conversation in which you are one party, it's probably legal even though the law seems to require one to send a beep down the lines every 15 seconds to notify all other parties that their conversation is being recorded. However, unless you have a court order or work for Ma Bell, you cannot legally record phone conversations to which you are not a party - even if you own the phone and one of the other parties is your minor child or spouse! This provision seems to be satisfied by simply informing those who use your phones that their phone conversations are subject to being recorded by you whenever you feel required to do so.

Although the Carterphone Supreme Court decision indicates that you can legally attach anything you want to your own phone lines as long as it does not interfere with communications or the operation of the phone company, for years, Ma Bell required folks to pay for special interfacing equipment to do so (even though they didn't use this same interfacing equipment on their same-designed equipment).

The Shriek option is probably illegal. It is YOUR decision when/if to use it. We would use it only as a last resort - only when the police and Ma Bell can't or won't stop the offensive calls after we've repeatedly complained to them - or to punish an intruder using an infinity bug. The Shriek option clearly has illegal applications. For example, some toadclone has been hassling you at your work, or a bill collector, or an ex-something or another. One could call him/her up about 3:00 AM. Then mumble something over the phone to get him/her to press the receiver tightly to the ear. Activation of the Shriek Circuit should then produce a sharp, stabbing pain in the ear.



- 2N4391 Or Equivalent N-Channel FET. R1 Must Be Adjusted.
- 100 K - 250 K 15-Turn Pot. Tuned So That $V_s = 0.65 \cdot V_{dd}$.
- 500 K Potentiometer Turned Until Output is Sharpest.
- 5 ohm-5 ohm Audio (Speaker) Transformer, 50 mA (Min.).
- 120 VAC Step-Down Power Transformer, 500 mA (Min.). Secondary Voltage According to Selected 78XX.

Figure 2: Basic TELERECORDER with Shriek Circuit and Power Supply.

Figure 3: Automatic (Auto.) Feature (Off-Hook Detector and Recorder Switcher).

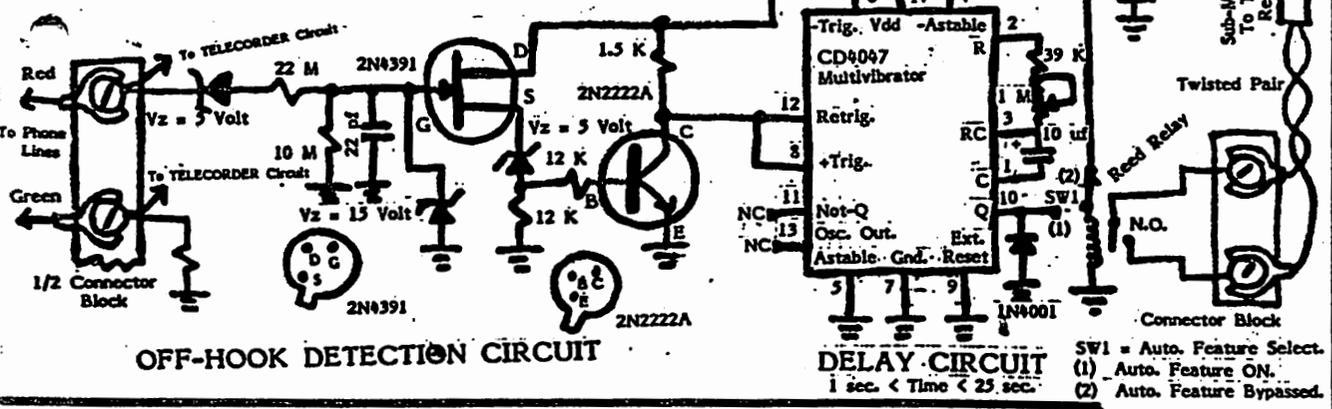
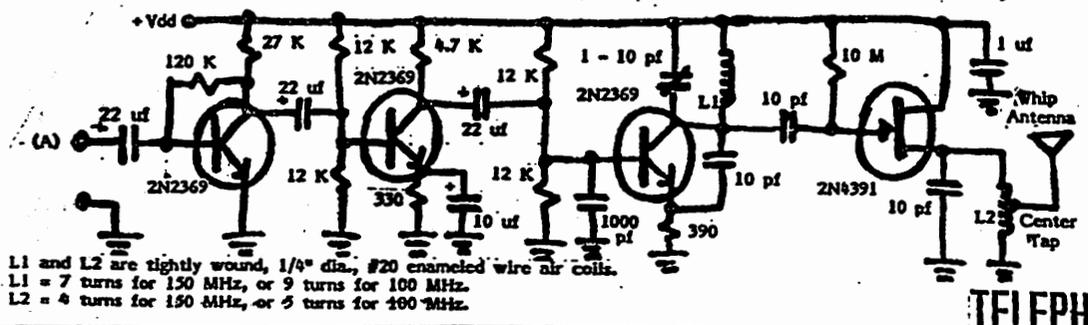


Figure 4: RF Transmitter with Audio Amplifier Stages.



- L1 and L2 are tightly wound, 1/4" dia., #20 enameled wire air coils.
- L1 = 7 turns for 150 MHz, or 9 turns for 100 MHz.
- L2 = 4 turns for 150 MHz, or 5 turns for 100 MHz.

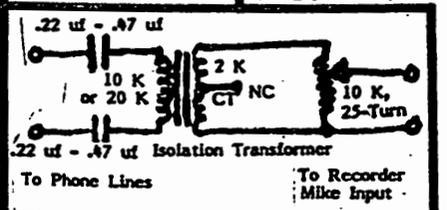


Figure 5: Typical Crude Commercially Available Telephone Recorder Interface.

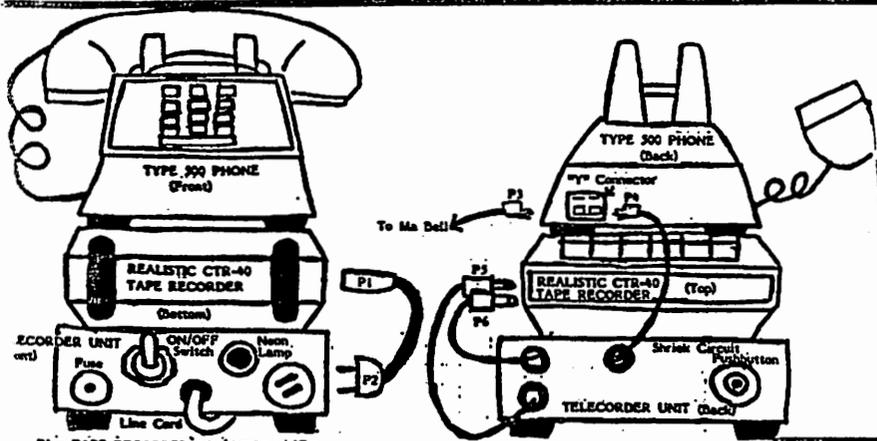


Figure 6: Physical Layout We Selected.

- P1 - TAPE RECORDER AC POWER INPUT
- P2 - TAPE RECORDER PLUG
Plugged into TELERECORDER II Auto. Feature is not installed, else into wall outlet.
- P3 - PHONE LINE PLUG
- P4 - PHONE PLUG FROM TELERECORDER
- P5 - AUX. INPUT TO TAPE RECORDER, MDG-PHONE PLUG
- P6 - REMOTE INPUT TO TAPE RECORDER, SUB-MINI PHONE PLUG
Installed only if Auto. Feature is installed.

DETECTING BUGS & TAPS

Many years ago, one could easily detect a phone tap/bug by listening to strange clicks. Some phone taps/bugs were even so crude that they tripped the 40 ma relay at the Central Office, causing Ma Bell service personnel to rush to the incriminating site. Others required that the tap/bug had to be constantly personally monitored. Except in TV thrillers, B movies, comic books and with some cheap detectives, these crude types of taps/bugs no longer exist. Today's taps and bugs cannot even be detected using sophisticated electronic techniques, not to mention audio observation.

The following are effective procedures for ferreting out almost all taps and bugs. It is best to first run these tests on the system after careful and detailed physical inspection is made to assure that the system is free of taps and bugs. Then, periodically retest the phone system. Even minor changes can detect the presence of taps/bugs. Always record all test results:

1) TESTS DONE WITH THE PHONE LINES DISCONNECTED AT THE SURGE PROTECTOR

(A) OPEN-CIRCUIT: An ohm meter is placed across the open-circuited red and green lines. Resistance should measure at least 1 Meg. ohm. If resistance is less than 1 Meg. ohm, or the meter's needle bounces around or drifts slowly upward (capacitive charge-up characteristic), a parallel tap/bug is indicated.

(B) SHORT-CIRCUIT: Place a temporary jumper across the phone lines at the surge protector disconnect site. Measure the resistance across the red and green lines at the most distant phone. The resistance should be 1 - 2 ohms. If resistance is higher, than a series tap/bug or drop-out relay is indicated.

(C) AUDIO GENERATOR: This test is done with the phone lines open-circuited. An audio frequency generator is connected to the lines through a series 22 K ohm resistor. A dual-trace oscilloscope is hooked-up with one input across the phone lines, and its other input across the audio generator. One trace on the CRT is placed over the other. The audio generator is then slowly swept between about 10 Hz and 50 KHz. If any notching or peaking effect different than your original clean test of the circuit is noticed - even a minor change - the presence of a tap/bug is indicated.

2) TEST DONE WITH THE PHONE CIRCUITS NORMALLY HOOKED-UP:

(A) Place a high-impedance voltmeter across the red and green lines. If the voltage drops to 5 - 6 volts while the phone and all of its extensions are hung-up, an infinity bug or similar type device is indicated.

(B) If the phones are hung-up and the voltage is less than the 48 volts or so expected for your area, a parallel tap/bug is indicated.

(C) If a phone is off-hook, and the voltage is higher than the expected 5 - 6 volts, a series tap/bug is indicated.

(D) Phone your test phone sometime when you know no one will be there to answer it (or tell them not to answer it). Use an audio generator with an automatic sweep from about 20 Hz to 20 KHz. Acoustically couple your audio generator to the phone you use to place the call. If the ringing of your test phone inexplicable stops at any frequency, an infinity bug is indicated. Most modern infinity bugs are dual-frequency turn-ON and single- or dual-frequency turn-OFF. Dual-frequency bugs can't be detected with this test. Still more sophisticated infinity bugs require an encoded signal for activation.

3) MICROPHONE TEST: Remove the mike from the phone. Inspect it. If it appears to be unduly thick or heavy, is soldered, or does not make a sound when you shake it (carbon granules), it is probably one of the popular drop-in mike bugs that has a built-in RF transmitter. Now test the mike terminals in the handpiece, pressing down on the hookswitch. Any voltage indicates some sort of hook-switch bypass device in operation.

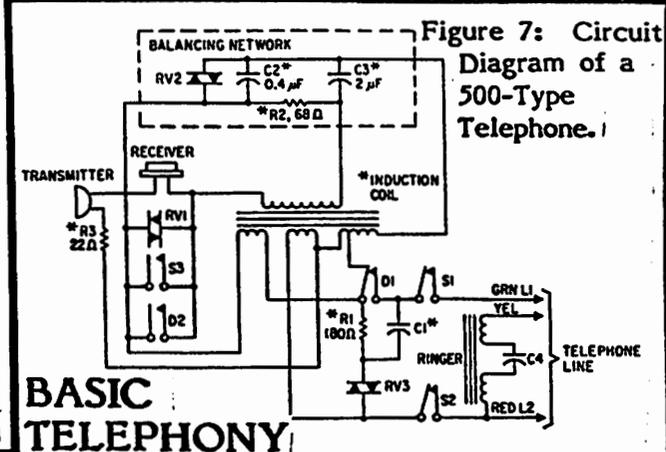


Figure 7: Circuit Diagram of a 500-Type Telephone.

BASIC TELEPHONY

Figure 7 is a schematic of a Type-500 Telephone - one of the most common telephone in use, and comes in various configurations. Sound is picked-up by the microphone (transmitter) in the handpiece. A small amount of this sound is fed back into the earphone (receiver) to provide the live sound of the phone. The rest of the sound-energy is sent down the phone-lines to the party you are phoning. This sound is amplified on the way at the phone company Central Office and by line repeaters. No amplification occurs in the phone itself.

RV1 (varistor) is used to suppress dial pulse clicks so they are not fed into the receiver. RV2, C2, C3, R2 and the windings of the induction coil form a hybrid arrangement that provides simultaneous two-way operation over a two-wire circuit. C1 and R1 compose the dial pulse filter to suppress high-frequency interference to nearby radios and TVs. R1, RV2 and RV3 also serve to reduce the efficiency of the transmitter on short loops from the central office to provide satisfactory transmission volume. All components marked with an asterisk (*) are located within the Telco network block located inside ITT, Western Electric and other phones (in still other phones, these components are on a PC board).

Most phones require three wires - red, green and yellow. In some phones, the green and yellow lines are jumpered together. The red and yellow wires make the phone ring. A 60 - 90 volt 20 Hz signal is applied to the ringer (two coils in series with a capacitor C4); C4 and these coils are designed so that once the phone starts to ring, it continues to ring while drawing very little current.

Although the ringer is connected to the phone lines at all-times, the rest of the phone is only connected when the handpiece is lifted off of the hook-switch. Ma Bell can determine how many phones you have on-line by either silently measuring the capacitance of the lines or the amount of current drawn during ringing. The specific impedance value of each ringer depends upon the phone used, but it is in the 1 Meg ohm range at 20 Hz resonance (measured at the Central Office).

If one were to tap the phone lines using a typical, commercially-available recorder interface or other tap/bug, Ma Bell (and thus the police) could easily electronically detect the foreign device attached to the lines by the substantially increased line loading. Thus, if you want to keep your business private, you require a device like the TELERECORDER with an ultra-high input impedance (infinite DC resistance, 30+ Meg ohm AC). The TELERECORDER is virtually undetectable electronically even if the lines are rung out with all of the phones and Central Office disconnected, using the most sophisticated equipment available! Its impedance is so extremely high that it is in the range of normal line leakage. The TELERECORDER is also virtually indestructible if some neanderthal tries to clear the lines with power pulses.

When the handpiece is lifted off of the hookswitch, switches S1 and S2 close while S3 opens. Closing S1 and S2 places the remainder of the phone into the circuit. Its impedance is 600 - 900 ohms. The 48 - 60 volts across the lines immediately drops to 5 - 6 volts.

To dial a phone number using a rotary dial, the lines must be interrupted (opened and closed) at a repetition rate of 10 pulses/sec. D1 is located in the back of the phone dial, and is used to produce these pulses. If the number 4 is dialed, D1 will open and close four times. During this entire interval, D2 remains closed so that the dial clicks are not fed back into the receiver. In fact, D2 remains closed during any duration that the rotary dial is away from its home position. For tone phones, the dial tones (two for each button) are sent down the lines, and detected at the Central Office. Tone phones have a drop-in block consisting of the pushbuttons and the contacts that are closed when they are pushed.

REFERENCES

- 1) TELEPHONE ACCESSORIES YOU CAN BUILD, and MORE TELEPHONE ACCESSORIES YOU CAN BUILD, Jules Gilder, Hayden, 1976 and 1980. Highly recommended. Many excellent circuits and ideas.
- 2) TAP NEWSLETTER, Technical Action Party, 1971 - 1984. No longer available, published or in business. THE AUTHORITY on technology mischief - particularly phones. Coined the terms "Phone Phreak" and "Ma Bell is a Cheap Mother." Detailed information on Red, Blue, Black, etc. phone boxes. Available only from CONSUMERTRONICS CO., P. O. Drawer 337, Alamogordo, NM 88310, \$2 per back issue. Sorry, no index is available.
- 3) CONSUMERTRONICS CO., P. O. Drawer 337, Alamogordo, NM 88310. SUPER-SURVIVAL CATALOG only \$1. 60+ technical survival publications on weapons, energy, phones (TONE DEAF), computers, electronics, financial, medical, etc. - all hard-hitting - some controversial!
- 4) BASIC TELEPHONE SWITCHING SYSTEMS, BASIC CARRIER TELEPHONY, and BASIC ELECTRONIC SWITCHING FOR TELEPHONE SYSTEMS, David Talley, Hayden, 1969, 1977, 1973. Excellent primer on telephone macro-systems but much of the information is dated.
- 5) Many fine how-to-do books are available on electronic surveillance from MENTOR PUBLICATIONS, 135-33 No. Blvd., Flushing, NY 11354 (catalog \$1), and LOOMAPRONICS UNLIMITED, P. O. Box 1197, Port Townsend, WA 98148 (catalog \$2). Especially highly recommended are:
 - (A) THE BIG BROTHER GAME, Scott French, 1976.
 - (B) ELECTRONIC SPYING and its accompanying PORTFOLIO OF SCHEMATIC DIAGRAMS FOR ELECTRONIC SURVEILLANCE DEVICES, MENTOR, 1979.
 - (C) WIRETAPPING AND ELECTRONIC SURVEILLANCE, National Commission For The Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance, 1976.
 - (D) BUGS & ELECTRONIC SURVEILLANCE, DESERT PUBLICATIONS, 1976.
 - (E) METHODS OF ELECTRONIC AUDIO SURVEILLANCE, David A. Pollock, Thomas, 1979.
 - (F) HOW TO AVOID ELECTRONIC EAVESDROPPING AND PRIVACY INVASION, William W. Turner, Investors Information Service, 1972.

THE VOICE DISGUISER

Copyright © 1981, JOHN J. WILLIAMS & FAMILY — ABSOLUTELY ALL RIGHTS RESERVED

BY: JOHN J. WILLIAMS, M.S.E.E.

SOLD FOR EDUCATIONAL PURPOSES ONLY

CONSUMERTRONICS CO. P.O. DRAWER 537, Alamogordo, NM 98310

I. INTRODUCTION

ALL PATENT RIGHTS ARE RESERVED

"Voice Disguiser" was the most eye-catching name I could think for this device and publication — even though it may incorrectly imply that the device has devious uses only. I have heavily concentrated on voiceprint analysis in this publication at some sacrifice to the other applications because the defeat of voiceprint analysis as evidence has always been one of my goals and the other applications are self-explanatory and straightforward. All of the applications include:

- A. Disguising one's voice to certain conversations that the speaker, for reasons of his own, wishes to remain private and anonymous.
- B. To aid those with soft voices and to assure one being heard in a crowd or where life or property may be in danger. With an addition of a front-end cone, this device makes into a bullhorn.
- C. To accommodate the hard-of-hearing, particularly the tone deaf.
- D. For harmless practical jokes. As a conversation piece. As a party pleaser.
- E. To provide audio outputs for computers and computer games, in conjunction with an oscillator.
- F. As a child's walkie-talkie or space communicator type toy.
- G. To filter out unwanted noise such as hums and whistles.
- H. To compensate for some voice deficiencies. Settings on this device will change a heavily bass or gruff voice, or a shrill, high-pitched voice into more normal sounding voices.

NOTE: We do not sell components or equipment. Because of experiences we have had with goons in the past posing as concerned customers, we also do not provide specific construction or use advice or the names of people who will "do it for you." This publication is sold FOR EDUCATIONAL PURPOSE ONLY. We also do not recommend the use of this device to offend anyone under Civil Law statutes.

Perhaps the main objective of this publication is to popularize voice disguisers to the point that it brings an end to the admissibility of voiceprint analysis as evidence. It is a dangerous and tyrannical practice that must be stopped! Whatever aid and comfort this publication may give criminals is far outweighed, in my view, by the freedoms for everyone preserved. Justice is not served by voiceprint evidence as both guilt and innocence can be proven with it regardless of which is true. Even though voiceprint analysis is based upon sound scientific principles, when it is claimed that it will consistently identify with reasonable certainty the identity of any voice, its credibility is the same as that of palm reading. I am not impressed by the so-called preponderance of evidence for voiceprint analysis.

II. VOICEPRINT ANALYSIS

Voiceprint analysis is generally the frequency spectrum analysis of one's voice. This technique has been used for 40 years and is described in engineering text books as "Spectrum Analysis," "Fourier Series," "Power Spectral Density," etc. Essentially, no matter how complicated any waveform is, it can be defined by a Fourier Series — that is by the summation of sine functions of various magnitudes, frequencies and phases.

Voiceprint analysis is not limited to the entire speech bandwidth (BW) for any utterance. An "utterance" is defined as any conversation or part(s) of any conversation arbitrarily chosen by the voiceprint analyst. Of course, when properly done (which is seldom, if at all), the comparisons are made between the tape recordings of the criminal and the suspect using virtually identical set-up, equipment and tape. Some other examples:

- A. Both sets of recordings are compared in the time domain for the utterance.
- B. A narrow BW component is compared between both sets of recordings throughout the utterance. Similar comparisons are made for other narrow BW components.
- C. Two or more narrow BW components are compared between each other for each recording for the utterance and the cross-compared with similar samples for the other recording.

What is meant by "compare" is that a statistical analysis establishing the correlation and the error functions are made. The analyst can then say, "With a ___% certainty, the two recordings were made by the same voice."

III. FACTORS THAT IDENTIFY THE VOICE A TOTALY OVERCOME WITH THE VOICE DISGUISER

1. FREQUENCY SPECTRUM: Two methods of identification are permitted: A) Personal recognition, and B) Voiceprint analysis. The objective of the Voice Disguiser is to substantially change the magnitudes, frequencies and phases present in the Fourier Series in such a random fashion that the voice cannot be identified either by personal recognition or by voiceprint analysis.

B. PARTIALLY OVERCOME WITH THE VOICE DISGUISER

1. **PAUSES:** People pause differently when they speak. The investigator or expert witness identifies consistent or very unusual pauses in the recorded utterances and compares them to the speech pattern of the suspect. Unless the pauses are marked, the Voice Disguiser will likely distort pause characteristics to the point of defeating identification.

2. **ACCENTS:** The Voice Disguiser, thru frequency spectrum manipulations, tends to disguise all but the heaviest of accents. It may make an accent completely unidentifiable or mistaken as another kind of accent. By and large, its effectiveness depends upon how well known the accent is.

3. **SPEECH DEFECTS:** These are disguised about to the same extent as accents.

C. NOT OVERCOME WITH THE VOICE DISGUISER

1. **SELF IDENTIFICATION:** If one identifies himself as the owner of a voice, even though the courts have ruled that self-identification, in itself, is not conclusive evidence, it does cause one to become a suspect. No voice disguiser that permits intelligible conversation can help here.

2. **PERSONAL KNOWLEDGE:** One can identify himself even more conclusively by using or divulging personal knowledge that he alone or a relative few others would likely possess.

3. **UNUSUAL EXPRESSIONS:** If one is known for some unusual expression or even a usual expression said in some unusual or overly repetitive manner, identification of the voice can be made.

IV. MECHANICAL VOICE DISGUISE

Numerous methods have been used to mechanically disguise the voice. These include: A) Speaking in lower or higher tones, B) Speaking with an unnatural accent, mannerism or voice defect, C) Placing an object, generally to muffle the voice, between the speaker and listener, and D) Placing an object(s) in the mouth to garble the voice.

To some degree, all of these methods work because they obviously do alter the voice. However, they are theoretically less effective against voiceprint analysis than against personal recognition. In any event, many judges and juries have been made to believe that, even with the severest efforts to mechanically alter the voice, identity of the speaker can be made with "reasonable certainty." Keep in mind that mechanical voice disguise may leave substantial portions of the speech BW unaffected. Even where the BW is affected by such disguise, since the changes are basically (in theory) non-random and are predictable and repeatable, the real voiceprint can be reconstructed from the altered one. In reality, some randomness is introduced mainly due to positional changes between the speaker, listener and mechanical voice disguiser, however, it appears that courts tend to ignore such favorable evidence.

These shortcomings can only be overcome by an electronic Voice Disguiser that both randomly and substantially changes the voice spectrum thruout the conversation. Even if the criminal himself wanted to repeat the performance with full recall of all of his electronic settings, he would be unable to do so. It then becomes impossible for the expert witness to reconstruct the voiceprint without guessing.

Also, keep in mind that there exists already substantial case law regarding mechanical voice disguise. Generally, courts have not distinguished between one form of mechanical disguise over any other as far as the effectiveness of voiceprint analysis. No known cases exists regarding electronic disguisers and electronic disguisers can be made in many variations each substantially different that each case would have to be tried from the ground up.

V. QUALITIES SOUGHT

A. The most important quality of any voice disguiser is to make the voice unidentifiable by personal recognition or voiceprint analysis (some applications; in others, some recognition may be desired). Nor can the voice be reconstructed by experts based upon an analysis of its circuit design. This means that it must substantially alter the frequency content of the utterance in a totally random, unpredictable and unrepeatable fashion. Randomness can be made by manually changing electronic characteristics such as filter design, frequency or Q, or to automatically change them thru injection of some random signal. Both methods are applied to each of the designs found herein.

B. The second important quality is that the disguised voice still must sound natural and not bizarre or generated electronically (some applications; in others, a bizarre voice may be sought). Otherwise, the message may not be understood. Ideally, one wants all of the distortion and noise that results to sound as if it came from the recorder, phone system, etc.

C. The Voice Disguiser must use cheap, commonly available and simply applied components that can be packaged very compactly. It must also be battery operated with small quiescent current.

Note: Many people who might be expected to receive strange phone calls are trained to use delay tactics to keep the caller on the line, such as claiming that he cannot be understood. Also, voiceprint analysis can be made in the presence of substantially noisy backgrounds. Sophisticated filtering techniques can be used to lift a fairly good signal from noise that is periodic (eg. jackhammer) or repeatable (eg. radio broadcast), to produce a reconstructed voiceprint. Also, if a voice disguiser is associated

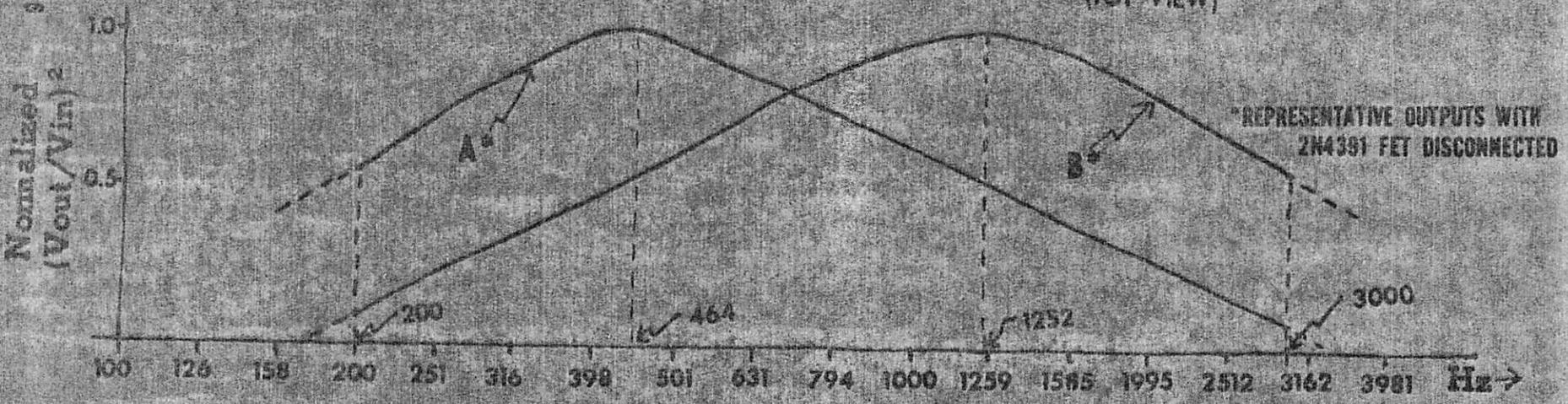
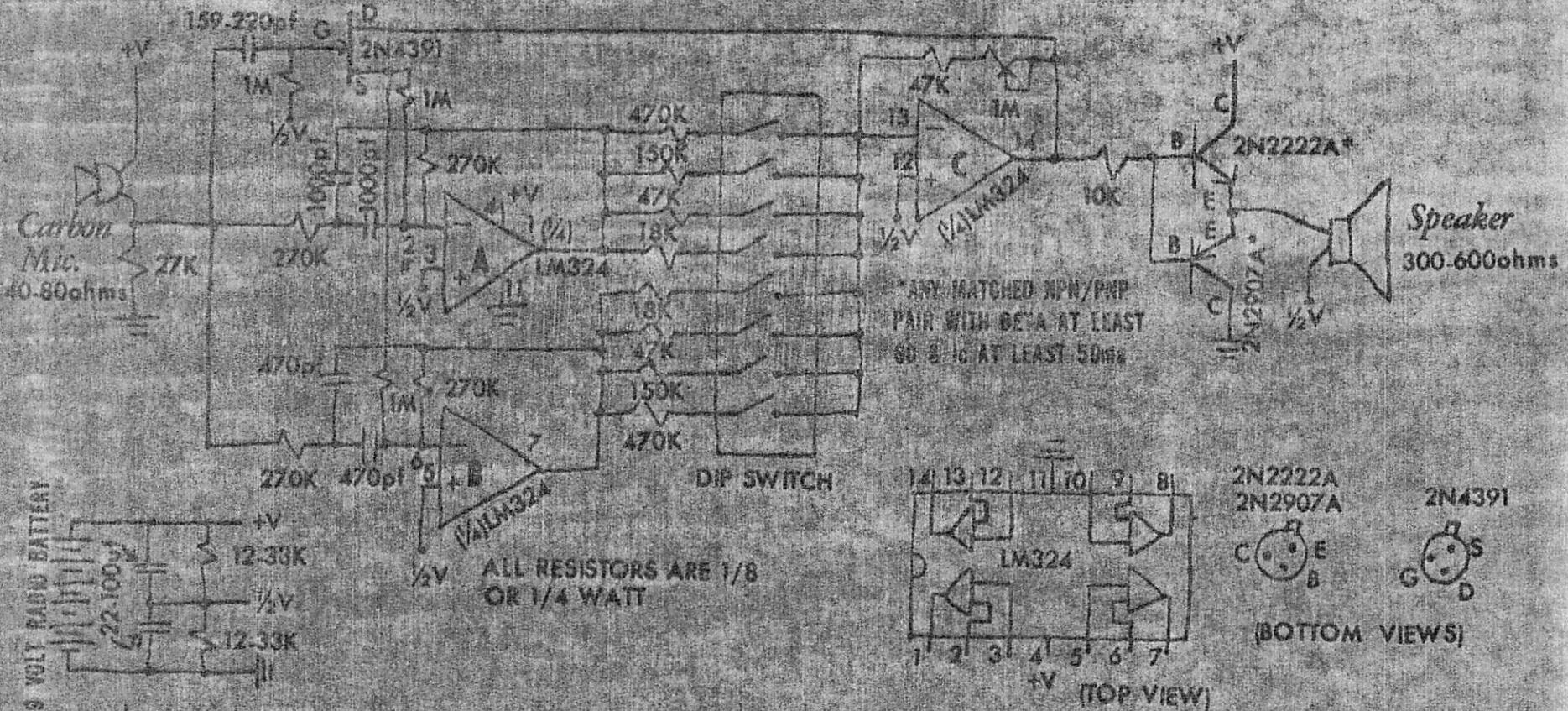


Figure 1 Dual Filter Concept.

with a call and the electronic voice disguiser does not have random, unpredicable and unrepeatable qualities, the expert can reconstruct the voiceprint by performing the inverse of the transfer function of the voice disguiser. Actually, phone circuits and tape recordings are, to some extent, electronic voice disguisers with so little randomness that they can be overcome by analysis (in theory).

VI. DESIGN CONCEPTS

A. DUAL FILTER CONCEPT

Essentially, this circuit consists of two wideband filters of Q (center freq./BW) of about 0.45 whose outputs are mixed in various combinations. Quiescent current for it (and the next design) is about 400 μ A. See Figure 1. Frequency plots are given. Notice, that no matter what filter (A or B) is considered and even though filter response changes with frequency, significant frequency content exists for all frequencies. If any frequency component were filtered to less than 1% of its input, it would give strong suspicion that an electronic voice disguiser was used, and if one was the only person known to have a voice disguiser that could spell trouble. By using very low Q filters, the lessening of any frequency component could be attributable to a natural lack of that component in the voice.

The DIP switch (8 pole) serves two purposes: 1) It varies the mixture of the two bandpass filters so that 255 combinations are possible from 100% Filter A to 100% Filter B, and 2) It also selects gains (the gain of C can be varied from 0.05 to 116), depending upon a combination of DIP switch and gain pot. settings. The gain pot. is used to adjust the gain to compensate for DIP switch setting and voice.

It is suggested that one picks out the best filter response to meet his needs. Then the gain pot. is adjusted for proper volume depending upon how loudly one expects to speak into the microphone and how loudly one expects the speaker to respond. Then, while the user talks, he continually flips corresponding DIP switch poles so that the A, B mixture, and not the gain, changes. For example, A is initially set at 18K ohms and B at 47K ohms. A is then switched to 47K ohms while B is switched to 18K ohms, then randomly back and forth during the conversation. Should the Voice Disguiser be ripped-off and associated with the conversation, no way could be used to reconstruct the voiceprint, except guessing!

The objective of the optional 2N4391 FET is to feedback a portion of C's output to either or both inputs. The amount of feedback is determined by the instantaneous high frequency content of the voice (about 700 to 4000 Hz). This feedback changes the Q and center frequencies of the filters automatically, randomly, unpredictably and unrepeatably. The 1M ohm FET Source resistances were selected by me to fit my voice, and DIP switch and gain pot. settings. They don't even have to be equal, but should be experimentally determined to allow changes within a desired distortion range.

The advantages of this circuit is that it is simple, inexpensive and does not suffer from great variations in filter Q s and center frequencies. Naturalness can easily be maintained. Also, one can get maximum effect by determining his most prominent frequency component and then tune both filters to be symmetrically and distantly spaced on each side of this component to eliminate its prominence in the voiceprint. Center frequencies are changed by varying the two filter capacitors or two 270K ohm resistors. The disadvantage of this circuit is that it suffers from such a low Q that some might feel that it does not change the voice enough.

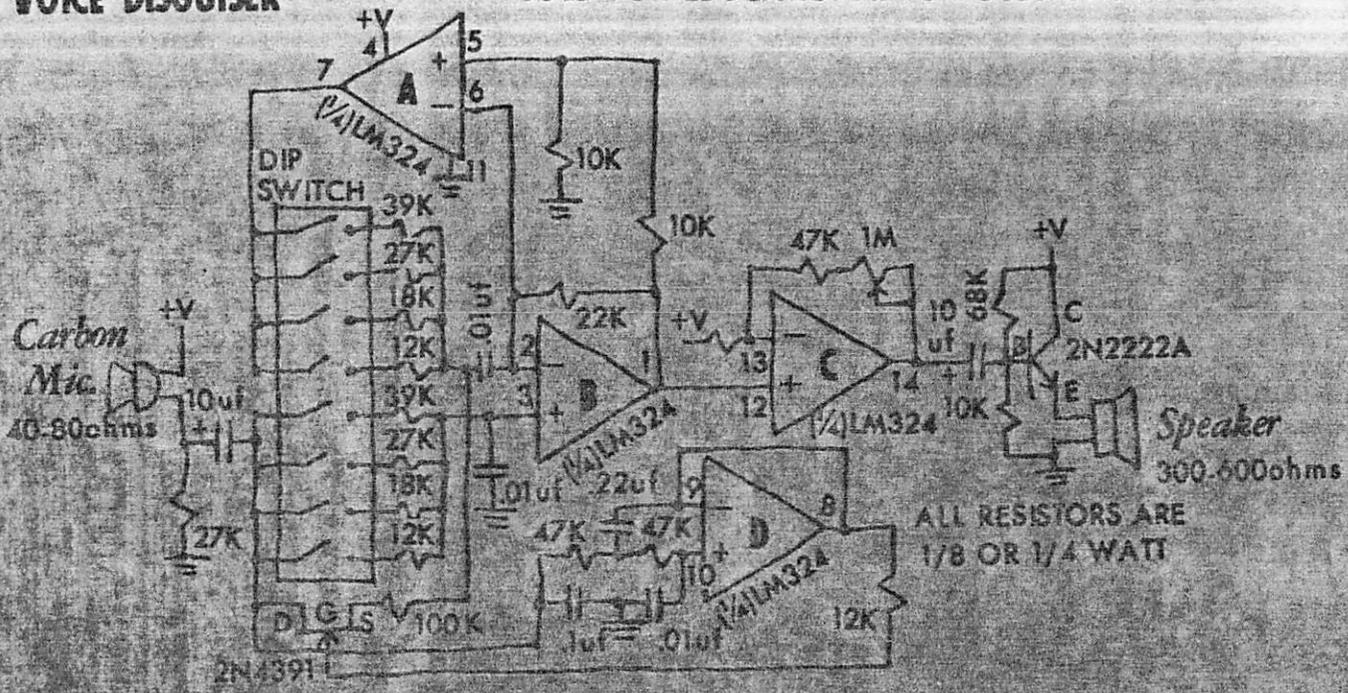
B. DUAL AMPLIFIER BANDPASS (DABP) FILTER CONCEPT

See Figure 2. This is a variable Dual Amplifier Bandpass (DABP) Filter, in which both Q and center frequency are varied by DIP switch settings. One of the best filter references around is: ELECTRONIC FILTER DESIGN HANDBOOK (Arthur B. Williams, 1981, McGraw Hill), and extensively covers DABP filter designs, as well as many other active and passive filter designs.

Op. Amps. A and B and associated circuitry makes the DABP filter. Filter gain is 2.0. Various center frequencies are set by the upper four DIP switches while various Q s are set by the lower four DIP switches. Center frequency equals the inverse of the upper setting resistance, the capacitance and 5.28 multiplied together, in this case around 470, 650, 920, 1290 Hz. Q equals the lower setting resistance divided by the upper setting resistance. Changing the lower setting changes Q only. Op. Amp. C is simply the output gain stage. Optional Op. Amp. D is a low pass filter (cutoff at about 100 Hz) used to modulate the FET, which, in turn, somewhat changes both the Q and center frequency in an automatic, random, unpredictable and unrepeatable fashion. The 100K ohm FET Source resistance suited my applications but should be experimentally determined for each case. This approach could have also been used in the above design.

The advantage of this circuit is that the spreads of Q s and center frequencies could be made quite large and can take on whatever values desired by the user. The disadvantages are that for large swings in Q and center frequency, output volume can change dramatically due to gross changes in what the filter passes. This circuit is also more complex, bulky and harder to operate.

I have given Voice Disguiser design much thought and research. Of course, the number of alternatives is very large - some using filtering; some, injection of random oscillations and/or noise; others, a combination. After a substantial amount of experimentation, I have come to the conclusion that these two alternatives (or similar ones) are the most effective for cost, size, battery dissipation and complexity. At some sacrifice of these qualities to obtain maximum effectiveness, the next design rates high.



RESISTOR VALUES PERMIT A Q OF 0.51 AND 3.3, AND CENTER FREQUENCIES OF 470, 650, 920 & 1290 HZ

Figure 2 Dual Amplifier Bandpass (DABP) Filter.

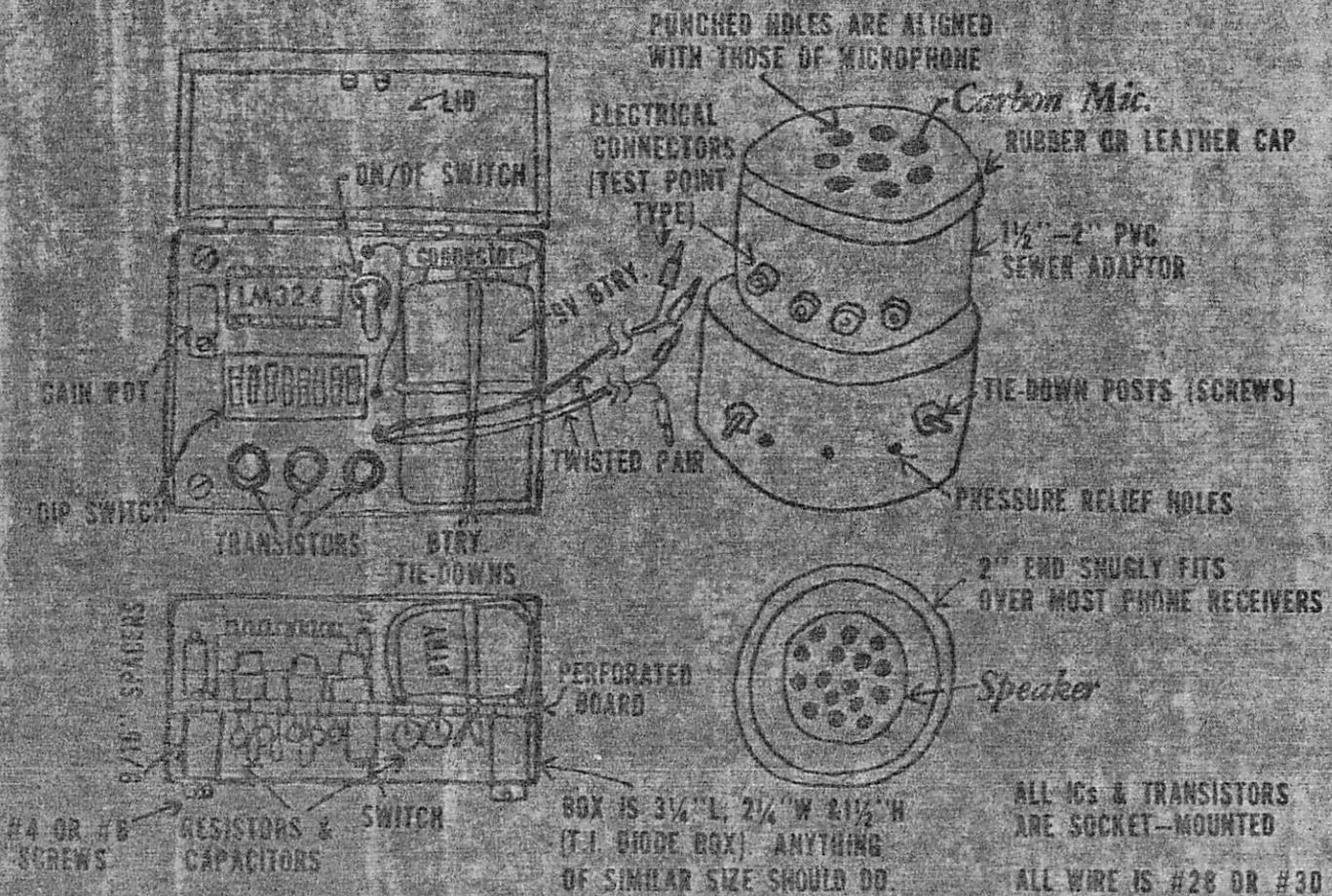


Figure 3 Construction Of Either Of These Concepts.

C. THE DELAY LINE CONCEPT

This method uses the Reticon Dual Analog Delay Line (SAD-1024A) to produce an adjustable phaser or flanger (variable comb filter). This very exciting approach is also very sophisticated and may be too complex for many experimenters. SAD-1024As can be obtained from Radio Shack for about \$12, accompanied by instructions and specifications. One might ask RETICON (345 Potrero Ave., Sunnyvale, CA 94086, 408-738-4266) for SAD-1024A application notes (No. 109, 104A, 119, 112 and especially 115). For about \$35, they will sell you an excellent evaluation board for it. The particular circuit that I have in mind is well described in Radio Shack's ENGINEERS NOTEBOOK, pp. 44-45, about \$2.50. By varying the oscillator's 1M ohm pot, its frequency is changed, thereby changing the comb filter notches. A randomly programmed FET can be placed parallel to this pot, to provide an automatic component to this randomness. The entire frequency spectrum is affected.

The advantages of this method is that once all the other pots, are set, varying the oscillator pot, is all that is required to play havoc with the frequency spectrum, naturalness is easily preserved even with substantial changes, and large volume differences do not result. The disadvantages are its great complexity, cost and bulk, and battery drain.

VII. DISGUISED COMPONENT VALUES AND IDENTITIES

In case your Voice Disguiser ever gets ripped-off - possibly leading to some gross misunderstandings, you should always remove the stampings on your electronic components. Solvents (such as paint thinner) are available; I prefer fine sandpaper or file. The schematic (this publication) may also get ripped-off so do NOT use the exact values I have shown but nominal values with wide tolerances and poor temperature characteristics. It takes a special effort to design something poorly on purpose to accomplish its desired function. If you build 10 Voice Disguisers, or a 100, each one should be substantially different. Also, each design should be somewhat based upon the voice characteristics of the end users. For example, for bass voices, the greatest randomness should be designed in at the low frequencies and the greatest amplification at the high frequencies. The opposite is true for high pitched voices. For mid-frequency voices, greatest randomness should be at mid-frequency while greatest amplification at both the high and low frequency ends. Of course, for some applications, the advise of this paragraph should be ignored. For example, if the Voice Disguiser is used to aid the tone deaf, then random changes should be very low and amplification should occur at the deaf frequencies.

Do not engulf the one PC or perf. board in epoxy, RTV, etc. Solvents are available that dissolve these away quickly while it becomes a real pain to make repairs or modifications.

VIII. THE MICROPHONE AND SPEAKER

An endless variety of microphones and speakers exists. I prefer the type used in phone handsets. They can be easily liberated and are rugged and compact. They also fit very nicely into PVC plumbing pipe, which is cheap and comes in many sizes and shapes. The circuits can be built into two assemblies (Figure 3) or into one. I prefer the former for size and security reasons, and for the ease of various circuits without having to build a microphone/speaker assembly for each one.

IX. CIRCUIT CONSTRUCTION AND USAGE HINTS

Figure 3 illustrates how I constructed and packaged the Voice Disguiser and is self-explanatory. After I tested the function of the mic./speaker assembly, I RTVed that assembly together. The speaker fits nicely into the bottom of the PVC adapter and rests on its ledge. I used a rubber cap on the top and several half-moon shaped rubber sections to separate the mic. from the speaker (cutouts provided for the jacks). The holes at the bottom reduce muffling for snug fits over phone receivers. If the fitting is not snug, tie-down posts are provided to attach the Voice Disguiser with rubber bands. I prefer a black housing (or dark grey) to reduce visibility by nosy passerbys.

The box assembly is built so that by simply removing four screws (bottom), the circuit can be removed from the box. The twisted pair leads are stored inside the box when not used. Two of the plugs connect to mic. jacks and two to speaker jacks.

The two assemblies fit easily into a coat pocket, valise, bag or hollowed-out book, and are quickly connected and mounted. Your initial settings and variations should be tested prior to any serious work. The variations are randomly made (some applications) during the conversation. Upon completion of use, wild setting should be made to stymie any goon. I enclose a very small screwdriver to facilitate DIP switch and gain pot. settings, inside the box.

The voice Disguiser can be used in reverse. That is the mic. end is placed over the receiver's speaker and the settings set to amplify the received voice while attenuating noise components.

Actually, I wasn't too thrilled with the connectors I chose, test point or tip type plugs and jacks. The reason why I chose them over mini-phone connectors is that the mini-phone jack interfered with the microphone and speaker (too wide). Unfortunately, the receiver speaker in both GTE and Western Electric phones is thick and to get everything to fit into that 1 1/2"-2" PVC adaptor required a very tight fit even with tip jacks. This adaptor is 2.125" long - anything longer is self-defeating because then your mouth doesn't properly speak into the Voice Disguiser. An alternative is to use in-line mini-phone connectors or other small connectors but I didn't care to have additional lines flopping around.

X. APPENDIX

A. WHY VOICEPRINT ANALYSIS AND TAPE RECORDINGS SHOULD NEVER BE USED AS EVIDENCE

Voiceprints should never be used as evidence! Some courts have been convinced by pseudo-scientific arguments from double-blind scientists with impressive credentials that voiceprints are as unique to individuals as are fingerprints. The theory goes that since no evidence is infallible, anything that looks impressive ought to be considered; further, that it is very unlikely that two people with identical fingerprints or voiceprints would have the same opportunity, motive and means for committing a crime.

My reasons against voiceprints are:

1. Frankly, I am not that convinced about the uniqueness of fingerprints, even though, no doubt, they are an order of magnitude more reliable than voiceprints. Every physical characteristic is defined by a gene arrangement. The number of gene arrangements, although quite large, is not infinite, and is generally not even known. Voiceprints are no different. People related by family, ethnic and racial backgrounds have greater likelihoods of having similar, if not identical, voiceprints. When someone clones you, you can almost always tell the race and sex of the caller due to genetic similarities in the voice forming structures.

2. Fingerprints can be seen and similarities and differences easily observed without much interpretation, and they are consistently repeatable. Voiceprints lack these qualities. BW distortion and noise characteristics of the voice, the air, all intermediate electronic circuits result in substantial deviations from perfection. Yet, courts have accepted voiceprint analysis based upon a) Recordings that are so poor that entire segments are unintelligible, b) Narrow bandwidth recordings improperly made with trashy tape and filled with distortion and noise, c) Recordings that are copies or reconstructed from copies, d) Recordings with erasures, unexplained gaps and possible splices, and e) Transcripts of recordings that no longer exist!

3. Voiceprint analysis requires that the suspect undertake recording sessions in which he is forced to repeat utterances used on the criminal tape, sometimes many retakes are ordered. He can be forced to repeat foul language and speech mannerisms alien to him - to even use a voice disguise method used by the criminal. The presence of legal counsel is not required.

4. The DA, in his anxiousness to railroad a suspect for personal gain, can have the voiceprint analysis conducted on all of the test tapes, comparing them to the criminal tape, until a close match can be made and ignoring all the dissimilar comparisons. Since the combinations of possible voiceprints analyzed can be extremely high, to rely upon only a few to establish proof is like identifying a culprit from 1% of one fingerprint!

5. It has happened more than once that the criminal tape is replaced by one test tape and then the voiceprint analysis is made between two test tapes! Keep in mind that voiceprint evidence is often used in sensational trials where much political gain or loss is at stake.

6. A person can easily be framed by having a perfectly innocent conversation changed by tape splicing to sound criminal. A copy is made of the spliced tape and voiceprint analyzed.

7. Voiceprints require the interpretation of "expert witnesses." These "experts", whose payment for testimony is based upon their "credentials" and how convincing they were in past cases, are generally listed in "Professional Witness" directories. They fall out to the side of the highest bidder - generally government, corporations and rich, big-shots. Right or wrong, they lack the evidence to support the side that pays their fee. You have seen how the defendant's bank of psychologists and psychia-

trists swear that he was insane at the time of the crime while the other side's pack swears to the opposite. Voiceprint analysts are similar circus performers. This is one way that justice is sold to the highest bidder. If you can't afford "expert" testimony to neutralize that of your opponent, expect to be railroaded!

8. The reliance upon recording equipment and tape is far too high. Refer to any audio electronics magazines that evaluate tape recorders and tape and you will find frequency responses that are not crisp and flat but roller coaster - sometimes with substantial peaks and nulls.

9. A voice mimic or simulator may have been used.

a) A professional mimic is hired to perform dirty tricks on people. No doubt, many innocent people have spent many years in jail, executed or murdered because of the naive acceptance of voice recordings and voiceprints as evidence.

b) With today's sophisticated electronic techniques, admittedly at some expense, a voice mimic or simulator can be designed. One approach is to duplicate the voice from scratch. Recordings of thousands of words are made of the target, thru bugs and wiretaps. From the recorded words, all the basic spoken sounds are catalogued for frequency content. The target's voiceprints can then be duplicated by a computer controlling a bank of oscillators (each gain is programmed by the computer). The various outputs are then mixed together to duplicate the voiceprint. This is automatically done in microseconds with no measurable change in the speech pattern. The computer then makes a terrorist phone call using the target's voice. 32 bit, high-speed microcomputers with 256K memories for just a few \$ Thousands will soon be here! Recent developments in IC technology has produced very powerful voice simulator chips. Computers now make phone calls to sell merchandise and take orders. This technology, once reserved for government, corporations and big-shots to frame their political enemies and highly controversial and outspoken people, is now in the reach of the TV repairman down the street! No one is now safe!

c) A second approach is similar to b) except that the voiceprint is reconstructed from that of another. A goon is hired to make a terrorist phone call. Everytime he speaks, the computer searches its memories to find the same word as the target would have spoken it. The computer controls a bank of very narrow-band bandpass filters. The frequency content of the goon's voice is then reconstructed to match that of the target.

d) Recordings can be made of the target until a very large vocabulary is acquired. The computer makes a terrorist call, programmed for the message. It then picks the required words and associated target voiceprints from its memories and combines them to make the message.

e) Actually, the Voice Disguiser can be made to roughly duplicate another person's voice, perhaps with some increase in its complexity this mimicry could be quite convincing.

10. In my opinion, voiceprint analysis violates the First, Fourth, Fifth, Sixth and Fourteenth Amendments. I should know better. Amendments apply to big-shots only!

The only way to destroy the admissibility of voiceprints in evidence is to so popularize voice disguisers that judges and juries must then consider the possibility that one was used in the case under consideration and that the real criminal's voice was very much different from that of the suspect.

B. ADDITIONAL LEGAL POINTS RELATING TO VOICEPRINT ANALYSIS

I am NOT a lawyer. However, using my local county law library, I have done some research into applicable law. Looking at ALP 34 (p. 915-1), Amber 2d, Telecommunications §§208-216, and 29 Amber 2d, Evidence §§368-369, 381, 435, and 432). I conclude, in addition to my other legal opinions provided in this publication that:

1. The trend is towards greater acceptance of voiceprints as evidence. Earlier trials declared it inadmissible but, based upon subsequent research, two opinions have emerged: a) They are as infallible as fingerprints, and b) They should be admitted only to support personal recognition testimony.

2. The main scientific research to support the accuracy of voiceprint analysis was made by the Michigan State Police Dept. on over 34,000 voiceprints (a federally-financed study). Note that the apparent objective was to support the use of voiceprints as evidence. Similar studies by those with other prejudices could, no doubt, arrive at entirely different conclusions.

3. The identity of the voice may be established by circumstantial evidence only.

4. A taped conversation can be admitted as evidence even though the identities of its recorded voices have not been made. However, so far, the identities then must be established during

the proceedings.

5. A witness may identify a suspect's voice in several tape recordings in court without ever having personally met the suspect, as long as that fact is brought out.

6. Before a tape recorded conversation can be admitted into evidence, generally, the following requirements must be met: a) A showing that the recording device was capable of taking testimony, b) That the operator of the device was competent, c) Establishing the authenticity and correctness of the recording, d) A showing that no changes, additions or deletions have been made, e) A showing of the manner and preservation of the recording, f) Identification of the speakers, and g) A showing that the testimony was made freely without threat or inducement.

7. A phone conversation can be taped by the phone company just about whenever it suits them, or by anybody else as long as the other side agrees to it, and is admissible as evidence. Except for emergency numbers, a beep is supposed to notify conversants of the recording but don't depend upon it.

8. Wiretapping and bugging by government entities need not necessarily require a court order and may be admissible as evidence even when it violates the agency's rules and regulations.

9. Obscene, threatening or harassing phone calls can bring up to 1 year in prison and/or up to \$1,000 in fines for the first offense. Subsequent offenses inflate the penalties to 18 months and/or \$5,000. Generally, when a person is harassed by such phone calls, he contacts the phone company. After three or so such calls are received, the phone company puts a tap on the line. The tap prevents the line from disconnecting when the caller hangs up (just as long as the called person doesn't). The phone used by the caller is thus determined. If it is from his home, business or place where he is easily recognized, conviction becomes routine. If from some other pay phone, unless he hangs around until the police arrives, conviction may be very difficult. Taps may be applied to some V.I.P. phones on a continuous basis.

REBEL ONLY \$7
RENTAL EQUIPMENT ONLY \$7
SURVIVAL GUNS & ARMS ONLY \$19
SILVER FOX GOLDEN ONLY \$19
MUGGER, KAPISIT-DEE ONLY \$13
EXPLOSION OF FACT TALK ONLY \$8
THE TESLA CONNECTION ONLY \$4
YONGE BEAT ONLY \$6
COMPLETELY DISMISSED & BELIEVABLE ONLY \$5
STOPPING POWER METERS ONLY \$8
NEWER METERS BOOK ONLY \$9
REPLETION ONLY \$4
HEAT X-CHANGER ONLY \$5
LOADPENER ONLY \$6
ADVICE METHOD BOOK ONLY \$10
CASIO' ALICE ONLY \$10

... (Detailed descriptions of each item follow in columns) ...

CONSUMER ELECTRONICS CO.
 P.O. DRAWER 637
 ALAMOGORDO, N.M. 88310

AUTOMATIC TELLER MACHINES

THE MOST VIZING PUBLICATION THAT CONSUMER ELECTRONICS OFFERS... THE MOST VIZING PUBLICATION THAT CONSUMER ELECTRONICS OFFERS... THE MOST VIZING PUBLICATION THAT CONSUMER ELECTRONICS OFFERS...

SOLD FOR EDUCATIONAL PURPOSES ONLY

SHOPLIFTER!

SHOPLIFT! is finally here! The unspeakable subject is addressed in full. Many methods are discussed in detail, including the classification of Universal Product Codes. Learn the truth about shoplifting, how it's done and the Business Community lies and cover-ups to avoid shoplifting. ONLY \$5.

GARAGE SALES & FLEA MARKETS

INFLATION EATING YOU ALIVE? CAN'T AFFORD WHAT YOUR DAD COULD BUY? YOUR AGE AND 10 TIMES THE INCOME? TYPICAL OF SALES TAXES? Many people now find that garage sales and flea markets are the answer. This pamphlet completely describes how a professional garage sale/flea market shopper saves a hundred dollars worth by the way shopping at garage sales and flea markets using a systematic and efficient approach. SHOP LIKE THE PRO! ONLY \$4.