los angeles FREE PRESS

HOW TO TELL IF YOUR PHONE IS RIIGGED vale privacy? have to be utt that. (Parenti

ART KUNKIN President Johnson would like us to believe him again, This time he passed the Omnibus Crime Bill



"MOUTHPIECE" BUG

\$125.00

saying that the government would not engage in the increased wiretapping that the new law permits, How can anyone believe that?

The Internal Revenue Service, the Attorney General's office, the FBI, and the CIA have wire-tapped even when the law did not permit them to do so. This is not a supposition; it is public record in many court cases over the last few years. Are these agencies, and all the others, going to stop when the law invites them to invade privacy? Americans would have to be utter fools to accept that. (Parenthetically, the one good thing Establishment falsehoods accomplish is that they turn true believing fools into anti-establishment sceptics).

If a law is passed giving officials more power over the humans they rule, they are going to use that law. That's a reasonable starting point!

The next question, therefore, is: What can we do now that Big Brother is officially in the business of electronic snooping, preparing the FBIcomputer to spew forth all those bad social security numbers on The Day of The Camp? What do we do now that the Omnibus has arrived and we're about to be taken for a ride?

It seems to me that it's essential not to panic just as it's important not to passively take that ride. Electronic surveillance of a home or office may cost many thousands of dollars for a single installation. Most people won't be directly affected and those that are can make the privacy invasion singularly unprofitable for the snoopers.

Of course, in the film, "The President's Analyst," the phone company obviously has every single phone bugged. But since this is a pluralistic capitalist country and not a movie set, a slight exaggeration is involved.

Unlike Europe, in the United States, a profitable public utility like the phone company is not nationalized; here we only nationalize the unprofitable ones like the post office. So the phone



HEAR THROUGH WALLS WITH HI-GAIN CONTACT MIKE \$97.50

company and the government face each other as equals (one a little more equal than the other), and I suspect it will still take some time, and we will be able to observe the process, for government agents to operate with total bureaucratic abandon in the telephone exchanges. They don't yet.

Not riding the Omnibus passlvely requires that we acquire some technical education about electronic surveillance and counter-surveillance. Anti-bugging, anti-snooping, anti-finking, antiduping. The key word is: Privacy. And, surprisingly, we're going to discover that there are simple answers to the snooping devices and that the best are the human head, the human heart and the closed human mouth.

Our information for this ar-

JUST IMAGINE.... FULL TELEPHONE SURVEILLANCE FROM THOUSANDS OF MILES AWAY

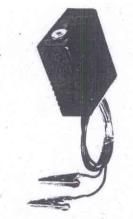
ticle comes, primarily, from a booklet titled, "How to avoid electronic eavesdropping and privacy invasion," available in its valuable totality for \$2.98 from Investigator's Information Service, 806 So. Robertson Boulevard, Los Angeles, Calif. 90035.

Investigator's Information Service also sells an "Investigator's Manual of Electronic Surveillance Methods and Devices" for \$12,50. This volume is larger, more complete, a veritable spy and espionage course. It points out that "a counter-measures technician beoomes an expert only when he is able to put himself in the position of the person who is making the bug installations,"

ISS also has a catalog of police and investigation equipment devices, giving specifications and prices for items they sell, including the de-bugging devices that we're going to mention, Isuggest you send them 25° if you want this catalog.

(Incidentally, ISS no longer sells wire-tapping equipment because of a new California law forbidding such sales to private citizens. They continue to sell de-bugging equipment and information).

Of course, by providing us with their information and granting us the right to paraphrase, quote, reproduce and summarize, they did not endorse, technically or politically, our paraphrasing or usuage.



AMAZING HARMONICA BUG \$395.00

There are two basic categories of bugging equipment: wired devices, which include hidden microphones, secret tape recorders and telephone tapes; and wireless devices, which include miniature radio transmitters, sound conduction equipment and exotic items like the "shotgun" and parabolic microphones, Detecting these two categories requires different approaches.

(Now this is obviously going to get technical in spots, Don't despair, Keep slogging along, We'll spice it up here and there with little bits of non-technical stuff that you will surely not want to miss. For example, did you know that at the time of the Sunset Strip ruckus a year and a half ago a police surveillance transmitter was allegedly found by visual inspection in Albert Mitchell's of-fice in the Fifth Estate Coffee House, when that was one of the prime centers for the organization of youth demonstrations, We have heard that the police never asked for their bug back and that now it is a pick-up in a guitar amplifier. Mitchell never knew about this bug, as it was appro-priated immediately by a well-known Chicago folk-singer).

Wired eavesdropping devices include any equipment utilizing a microphone physically connected by a wire to the actual monitoring device. This type of equipment is often easier to locate, de feat and destroy precisely because of the connecting wires.



LONG DISTANCE "SHOTGUN" MICROPHONE \$1295.00

Microphones can be hidden in electrical fixtures such as lamps, wall sockets, ceiling fixtures, or even radios, television sets, record players, and almost any kind of electrical equipment including appliances, Other good hiding places include: embedded in the wall and covered with putty, taped into desks, sofas, bookcases, hat

continued on page 3

NEW FEDERAL LAW PERMITS WIRE TAPS

signal generator which sends a high frequency audio tone through the suspected line. If the line is bugged the result will be an audi-

bugged the result will be an auch-ble squeal in the mike's diaphragm will vibrate. This unit, however, is not effective against carbon mike bugs as these have no dia-bles or

The counter-snooper should not make the mistake of assuming that only one bug was placed. If one bug is discovered, a thorough search must be completed, Fur-nishings, walls, floors, doorways, windows, ducts, everything in a

hismings, wais, noors, doorways, windows, ducts, everything in a room thought to be bugged must be checked. Other possibilities are pictures, calendars, books, shelves, cabinets, clocks, pens, pencils, and underneath desk

pencils, and underneam uses drawers. Newly placed pictures, rear-ranged furniture or different of-fice equipment all may be clues to the recent presence of eaves-

droppers. The widespread manufacture and sals of tiny eavesdropping

devices makes security from pri-vacy invasion a tricky proposi-

tion, Precautions against illegal entry help, Observation of alleged repairmen who ask for entry into

repairment who ask for entry into home or office helps. Since it is assier to bug than to de-bug, a householder or businessman must consider his security already compromised, should bugging be suspected in any way. In order to preserve that se-curity, some highly competitive businesses have gone so far as to install the "Fishbowl," which is a room within a room; a room with transparent walls, floor and cell-ing.

ing. In the interior of the "Fish-

In the interior of the "Fish-bowl" there are no lights, wires, tolephones or other electrical fix-tures. Other possible hiding places for bags such as water coolers, office equipment and coin operated machines are kept at a discrete distance outside the sound-proof shell. All furniture is either transparent placetiglass or moulded, unupholstered plas-tic

In each of the four walls of the

In each of the four walls of the "mother" room, inside which the security room is located, so called "white noise" speakers the effectiveness of any bug which may have somehow been hidden in the mother room. The plastic walls of the Fishbow! have a 20 decibel attenuation factor, thus reducing the usise isvel inside the security room to one suitable for confort.

for comfort. Transactions carried on inside such an installation are relatively bug proof, and the information discussed is then as secure as the people who share in it within the

people who share in 1 within the plastic room. However, other defensive and bess expensive procedures may be used by anyone discussing information they desire to be pri-vate. Radios turned on to full vol-ume, electronic noise generators, or even jury rigged noise makers — a small piece of cardboard placed so that the blades of an electric fan strike it—will all make enough noise to make con-versation in the room unclear as faras the eavesdropper is con-cerned.

cerned. In similar fashion, record play ers, television sets, electrical appliances, even bathroom show-ers turned on full force will mask important conversations in a di

important conversations in a dublous environment, Conversation may be more difficult but its se-

curity is more certain. The human ear can concentrate

on a single voice in a group con-

versation or in a noisy environ-ment; a microphone is unable to do this. It hears all noise, con-versations or otherwise within its

Wireless devices do not require

any physical connection between pickup device and monitoring unit pickup device and municoring unit (earphone or tape recorder). In this day of miniaturisation, the microphone, power supply and electronic transmitting circuit can be contained within a single

range.

tic.

ontinued from page 1 racks, drapes and acoustical tile. secreted in plants, mirrors,

or serveted in plants, mirrors, paintings, trophies, etc. Where there is more time to install a wired microphone, an entire strip of moulding may be removed and a small hole drilled to permit the installation of the mike, With the wires fished through the wall to an adjacent listenire nocet, and the moulding listening post, and the moulding replaced, it is virtually impossible to detect the tiny hole behind which the mike has been placed, This is where close visual inspec-

This is where close visual inspec-tion pays off. Given the time, a telephone expert can make a rather lear-some snooping device out of any phone. This is done by making a simple "ipmer" connection in-side with a piece of wire which transforms the handset into a hot mike" that will be an everpresent ear whether the handset is hung up or not.

up or not. After this connection is made, the eavesdropper makes a phone tap at any location along the line, The target of the second secon contact.

contact. There is also a Telemitter drop-in bug which is an exact duplicate of the inner microphone of the telephone into which a small transmitter has been built. By untransmitter has been built. By un-screwing the mouthplece and re-moving the existing mike, the snooper substitutes the drop-in and replaces the mouth cover. There is virtually no way the substitution can be visually noted.

substitution curve visually holed, except by dismaniling the scaled unit. The drop-in is a parasite, functioning off the current in the telephone line itself. It is so powerful that it oreeds no antenna to transmit 200 or 300 feet to be received by an ordinary FM re-ceiver on an unused band.

Installed in a matter of seconds, the unit need never be replaced, serviced or retuned. The ultimate serviced or retuned. The ultimate in modern devices, this unitwhich sells for \$125 (but may no longer be purchased in California) trans-mits both sides of a telephonic conversation, and, since it pulls the same current load as the real telephone mike, it is difficult to detect by voltage drop tests. (La-ter on in this article we will des-cribe tests that can be done with an FM receiver and a TV set to detect such equipment).

detect such equipment), Similar modifications can also be utilized in any home or office intercommunication system. The best protection against such an invasion is a careful visual in-spection of the entire wiring system. (The longer and more com-plex the wiring system, the easier

It is to tap). Literally every square inch of It is to tay, Literally every square inch of the suspected bugged area must be searched. The counter-intelli-gence agent should check any vis-ible irregularities such as a new patch of paint (particularly thin lines of sliver paint which may function as a printed circuit to wire a microphone, a blob of putty, cracks in the baseboard and floor board. All may be clues to recently planted bugs. Watch for places where soda straws, plastic tubing and spike microphones can be inserted holfwe, Soda straws and plastic tubing can be an acoustical con-tubing can be an acoustical con-

tubing can be an acoustical con-ductor inserted under doors or ductor inserted under doors or through window sills and termin-ating in a sensitive microphone. Check all ducts and outlets be-cause they often transmit sounds, Placing an amplifier, microphone or transmitter in such a duct would provide a snooper many bours of thormative literonin.

hours of informative listening. There is a simple and inexpen-sive device called a microphone case often much smaller than a pack of cigarettes. Some require no antenna, which further compli-cates the chance for the bug's discovered

cates the chance for the bug's discovery. Bugs have been known to be built into such things as clgarette lighters, ofgarette packs, fountain pens, beit buckles, brooms, paper cup dispensers, paper weights, books and sewn inside clothing. The ingenious private invesi-gator actually had a high powered bug built into the cup of a bras-siere, which was then worn by a female detective on a divorce case involving an over-amorus husband. Such installations are often used in industrial espion-age.

A bug can be hidden almost can expen-age. A bug can be hidden almost any-where. Experimental units now available using what is called an integrated circuit can be no long-er than one-quarter of an inch square, an eighth of an inch thick, and a securibuloss contain the and, nevertheless, contain the equivalent of ten transistors and equivalent of ten transistors and hirty or more resistors and ca-pacitors, For the sake of compar-ison, using integrated circuits, today's 17 inch portable TV set could be reduced to the size of a box of kitchen matches. Wireless bugging transmitters are usually tuned in to the 88 to 108 mc (megacycle) range, the standard commercial FM band, If a standard FM receiver is brought within the area of a transmitting device, and the receiver is slow-ly tuned through its entire range



It's the greatest fun idea in snooping in years! Concealed inside this innocent-looking toy is a tiny microphone and miniature wireless radio

The cute antennae are REAL antennae. They broadcast a strong signal to any FM radio within 100 feet WITHOUT CONNECTING WIRES! Any conversation within ear-shot of the bug will be heard on the radio, loud conversation and clear.

until the frequency of the bug is reached, the receiver will emita loud high pitched squeal or feedback.

ck. To discover the exact location

back. To discover the exact location of the device, the volume of the receiver is cut down each time feedback is heard and the search continued until the approximate location of the buy is determined, when a visual search is made. Since the more sophisticated FM ratios have several bands, it is possible for a complete sur-vey to be made of the frequency range on which a bug is likely to be transmitting. Almost any radiorepairman or electronics hobbyist can make a simple modification on a standard FM radio, adjusting the tuner's oscillator padder to allow it to to nearly 115 mc. Even if the bug is transmitting in the 30 to 50 mc range, harmoon-les may reveal its presence. A

ics may reveal its presence. A transmission at 38 mc, for ex-

ics may reveal its presence. A transmission at 38 mc, for example, will produce a resonant frequency feedback at the first harmonic, 76 mc; at the second harmonic, 114 mc, etc. Where no other anti-surveil-inance equipment is available, a standard television set is another excellent bug detector. In the area where wireless eavesdropping is suspected, the counter-intelligence investigator should first allow the set to warm up, then utri to Channel 2. When a tr set is used for antibugging, the outside antenna should be replaced with trabbit ears, which are then systematically moved about the area. If the fine turn ing knob is turned to its far counter-lockwise position. But yead on a strike the set of the set of the set of the set.

its far counter-clockwise posi tion, the TV set is tuned t frequency of approximately megacycles. By moving the fine tuning knob clockwise, the set is advanced to a frequency of 60 mc. Thus the investigator has moni-tored a total of 5 megacycles in the very high frequency (VHF)

If a signal is detected, there will be either a visual herring-bone pattern or an auditory feed-back squeal. If nothing is indica-ted, the Channel selector should be moved to Channel 3, the low frequency end of which is 60 mc.

The same tuning technique is re-peated as outlined for Channel 2. Beginning with Channel 2, the threstigator can "check out" the transmission spectrum between \$4 and 86 megacycles by mov-ing along the way—from Channel 2 to Channel 6. Beginning with Channel 7, the frequency then jumps to 174 mc. It is possible with this tedious technique, systematically "scan-

technique, systematically "scan-ning" the area with the rabbit ears at each frequency setting to cover up to 890 megacycle transcover up to 800 megacycle trans-missions. Athongh this is an un-likely range for most of today's modern surveillance equipment, the state of the art is rapidly developing and, in the counter-measures business, no possi-bility must be overlooked. Also, these high frequencies may pro-vide the investigator with a sim-ple method of picking up a har-monic of a much lower frequen-cy. cy.

There is one possible drawback There is one possible drawback to this seemingly simple proced-ure, if the eavesdropper is using a transmitter triggered on or off by a remote control and has reason to believe counter-sur-veillance is being used, he can simply turn off his bug and there will be no simeal to detect

will be no signal to detect. The catalog of Investigator's Information Service lists fairly inexpensive bug detectors which are more convenient to use than

standard FM or TV sets. The best possible protection against a wireless microphone is

its detection and removal, Built in systems to jam transmissions

are less effective and more cost-

ly. An experienced investigator may however, after reasonably determining that a room has been

determining that a room has been bugged, leave jamming or anti-bugging devices in the room until the hidden transmitters have been located by a complete physical search of the area,

Search of the area. For greater security, even af-ter a room has been searched, business firms holding top pri-ority conferences should make some provisions during such con-forences for the use of back-ground music or some jamming derice as a neon transformer. The problem with jamming de-vices is that they will not inter-fere with wired microphones and may interfere with legitimate FM broadcast transmission, pringing

broadcast transmission, bringing down the wrath of the Federal

Communications Commision,

.....

Telephone taps are often u

in connection with tape recorders which begin operating when the phone is lifted off the hook or people begin to speak over the

When a telephone tap is suspec-

When a telephone tap is suspec-ted, one of the most effective da-fensive moves is to dial the re-corded time signal. Once the signal nai begins, the voice-activitated bug will begin transmitting. If the unit is battery powered, the longer the time signal is permitted to re-pat its mindless course through-out the day, the lower the battery of the bug will run. If the device is running off tele-phone or house current, this pro-

phone or house current, this pro-cedure will, at least, be very ag-gravating to the eavesdropper.

Another defensive technique is to remove the handset from the

cradle, causing the dial tone to go

cradle, causing the dial tone to go out over the line, and activate the tape recorder. This measure is not effective in those parts of the country where an operator auto-matically comes on the line if a phone is off the hook for more than 30 seconds and number is not dialed

The use of an FM radio, or field

not dialed,

the set of the set of

One of the simplest, least ex-One of the simplest, least ex-pensive and most effective me-thods of checking for so-called ephonemics' installations on tole-phone and intercom systems is by obtaining a particular kind of induction coil called a "Snooper" from a police or detective quip-ment supplier such as the one described above. The most basic visual methods of checking a phone line for a tap is as follows:

is as follows:

Is as follows: Check the small terminal block on the wall. Three wires should be found running from the phone to this block, Remove this block from the wall and check for any additional wires which might be running from it into the wall. Also check the acrews and term-inals for scratch marks which could suggest the use of alligator clips. clips.

Check the outside pole for any wires which might be running down the pole, If possible, the pole itself should be visually checked since a wireless transmitter could be connected to a tap or an

could be connected to a tap or an induction unit and be hidden on top of the pole. Another defensive method gain-ing favor is that of using phone scramblers which convert tele-phone conversations into sounds unitedligible to anyone not having a similarly frequency matched scrambling unit. Several compan-tes specialize in the sale of this type instrument--which is battype instrument—which is bat-tery powered and portable. Once it is suspected that a

Once it is suspected that i phone is bugged or tapped, a phy-sical search of the instrument should be made, preferably by someone familiar with telephone circuitry for extra wires and the detect substitute mouth hard-to piece. If there is some suspicion that a telephone is hot-miked, it is wise to say nothing important in the vicinity of the phone until a radio, neon transformer or some ning device has been placed jam

next to it. Nor is it safe to discount the possibility of the Harmonica Bug, which shows the sophistication of the devices available to the eavesthe devices available to the eaves-dropper. Once this sub-miniature device has been installed inside the phone or anywhere between the instrument and the outside pole, this unit can be activated prom any place in the country. The eavesdropper need only dial the area code, then the first six digits of the bugged telephone number. At this point, he blows a tiny one-note harmonica or pitch

number, At this point, he dows a tiny one-note harmonica or pitch pipe (hence the name). The sound of the note generates a current which will activate the telephone. The phone will not ring; the hand-set while still in place on the cra-die acts as a security mirror. dle acts as a sensitive micro-phone and transmits over the phone line all conversations taking place in the room. This little goody used to be sold in California goody uses. for \$395.00.

Should an individual or a firm have reason to believe that a law enforcement agency is using elec-tronic surveillance methods to obtain confidential information, it is advisable to consult an at-torney. If private individuals are believed to be using these methods to gain information, there are four options: options:

1. Discrete dissociation with Discrete dissociation with those persons; 2. Direct confron-tation with the eavesdroppers;
Consultation with a law en-forcement agency; or, 4. Em-ployment of electronic countermeasures

This article has no end, it runs into and out of such books as Omar Garrison's "Spy Government, the emerging police state in America."

It is really not possible to be It is really not possible to be either optimistic or passimistic; it's just important that people know as much as they can and not give up. The right to a private, self-hulfilling life is still the goal and even becomes clarified in the face of the enemy...