LOS ANGELES FREE PRESS

Vol. 5 #26 (Whole #206)
In Two Parts
PART ONE

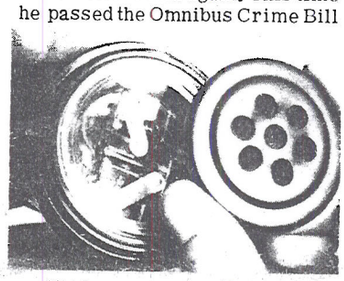
OL4-7100



# HOW TO TELL IF YOUR PHONE IS BUGGED

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 wire-tapping 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).

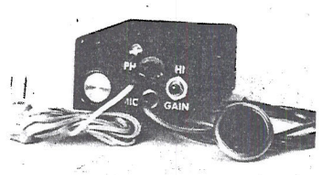
If a law is passed giving officials more power over the humans they rule, they are going to use that law. That's a reasonable starting point!

The next question, therefore, is: What can we do now that Big Brother is officially in the business of electronic snooping, preparing the FBI computer 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 passively requires that we acquire some technical education about electronic surveillance and counter-surveillance. Anti-bugging, anti-snooping, anti-finking, anti-duping. 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*

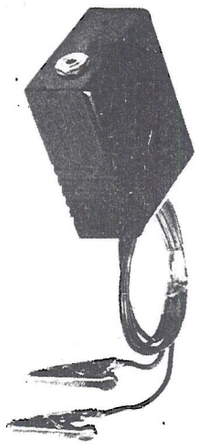
ticle comes, primarily, from a booklet titled, "How to avoid electronic eavesdropping and privacy invasion," available in its valuable totality for $2.98 from Investigator's Information Service, 806 So. Robertson Boulevard, Los Angeles, Calif. 90035.

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. I suggest 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.



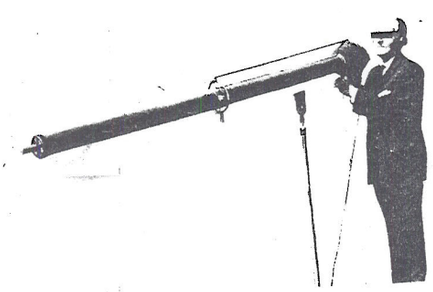
**AMAZING HARMONICA BUG**

**$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 office 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 appropriated 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, defeat 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

continued from page 1

racks, drapes and acoustical tile, or secreted 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 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 inspection pays off.

Given the time, a telephone expert can make a rather fearsome snooping device out of any phone. This is done by making a simple "jumper" connection inside 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.

After this connection is made, the eavesdropper makes a phone tap at any location along the line, inside the house or office, from the outside junction box or as far away as the phone company substation where the exchange for the phone is located. The two wires concerned, called the subscriber's loop, may be located visually or with the "buttinsky" (the special lineman's handset) clipped into the line randomly or by an induction coil which is placed next to a pair of wires and picks up the electrical impulses passing through without direct physical 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 unscrewing the mouthpiece and removing 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, except by dismantling the sealed unit. The drop-in is a parasite, functioning off the current in the telephone line itself. It is so powerful that it needs no antenna to transmit 200 or 300 feet to be received by an ordinary FM receiver on an unused band.

Installed in a matter of seconds, the unit need never be replaced, serviced or retuned. The ultimate in modern devices, this unit which sells for $125 (but may no longer be purchased in California) transmits both sides of a telephonic conversation, and, since it pulls the same current load as the real telelphone mike, it is difficult to detect by voltage drop tests. (Later on in this article we will describe tests that can be done with an FM receiver and a TV set to 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 inspection of the entire wiring system. (The longer and more complex the wiring system, the easier it is to tap).

Literally every square inch of the suspected bugged area must be searched. The counter-intelligence agent should check any visible irregularities such as a new patch of paint (particularly thin lines of silver 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. Drive a long nail into suspect holes. Soda straws and plastic tubing can be an acoustical conductor inserted under doors or through window sills and terminating in a sensitive microphone. Check all ducts and outlets because they often transmit sounds. Placing an amplifier, microphone or transmitter in such a duct would provide a snooper many hours of informative listening.

There is a simple and inexpensive device called a microphone signal generator which sends a high frequency audio tone through the suspected line. If the line is bugged the result will be an audible squeal in the microphone itself because the mike's diaphragm will vibrate. This unit, however, is not effective against carbon mike bugs as these have no diaphragm.

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. Furnishings, walls, floors, 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 drawers.

Newly placed pictures, rearranged furniture or different office equipment all may be clues to the recent presence of eavesdroppers.

The widespread manufacture and sale of tiny eavesdropping devices makes security from privacy invasion a tricky proposition. Precautions against illegal entry help. Observation of alleged repairmen who ask for entry into home or office helps. Since it is easier 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 security, 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 ceiling.

In the interior of the "Fishbowl" there are no lights, wires, telephones or other electrical fixtures. Other possible hiding places for bugs 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 plexiglass or moulded, unupholstered plastic.

In each of the four walls of the "mother" room, inside which the security room is located, so called "white noise" speakers emit a loud howl. This hampers the effectiveness of any bug which may have somehow been hidden in the mother room. The plastic walls of the "Fishbowl" have a 20 decibel attenuation factor, thus reducing the noise level inside the security room to one suitable 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 plastic room.

However, other defensive and less expensive procedures may be used by anyone discussing information they desire to be private. Radios turned on to full volume, 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 conversation in the room unclear as far as the eavesdropper is concerned.

In similar fashion, record players, television sets, electrical appliances, even bathroom showers turned on full force will mask important conversations in a dubious environment. Conversation may be more difficult but its security is more certain.

The human ear can concentrate on a single voice in a group conversation or in a noisy environment; a microphone is unable to do this. It hears all noise, conversations or otherwise within its range.

**********

Wireless devices do not require any physical connection between pickup device and monitoring unit (earphone or tape recorder).

In this day of miniaturization, the microphone, power supply and electronic transmitting circuit can be contained within a single case often much smaller than a pack of cigarettes. Some require no antenna, which further complicates the chance for the bug's discovery.

Bugs have been known to be built into such things as cigarette lighters, cigarette packs, fountain pens, belt buckles, brooms, paper cup dispensers, paper weights, books and sewn inside clothing.

One ingenious private investigator actually had a high powered bug built into the cup of a brassiere, which was then worn by a female detective on a divorce case involving an over-amorous husband. Such installations are often used in industrial espionage.

A bug can be hidden almost anywhere. Experimental units now available using what is called an integrated circuit can be no longer than one-quarter of an inch square, an eighth of an inch thick, and, nevertheless, contain the equivalent of ten transistors and thirty or more resistors and capacitors. For the sake of comparison, 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 slowly tuned through its entire range until the frequency of the bug is reached, the receiver will emit a loud high pitched squeal or feedback.

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 bug is determined, when a visual search is made.

Since the more sophisticated FM radios have several bands, it is possible for a complete survey to be made of the frequency range on which a bug is likely to be transmitting.

Almost any radio repairman or electronics hobbyist can make a simple modification on a standard FM radio, adjusting the tuner's oscillator padder to allow it to tune from approximately 70 mc to nearly 115 mc.

Even if the bug is transmitting in the 30 to 50 mc range, harmonics 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-surveillance 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 turn it to Channel 2.

When a tv set is used for anti-bugging, the outside antenna should be replaced with "rabbit ears," which are then systematically moved about the area. If the fine tuning knob is turned to its far counter-clockwise position, the TV set is tuned to a frequency of approximately 54 megacycles. By moving the fine tuning knob clockwise, the set is advanced to a frequency of 60 mc. Thus the investigator has monitored a total of 6 megacycles in the very high frequency (VHF) band.

If a signal is detected, there will be either a visual herringbone pattern or an auditory feedback squeal. If nothing is indicated, the Channel selector should be moved to Channel 3, the low frequency end of which is 60 mc.

The same tuning technique is repeated as outlined for Channel 2.

Beginning with Channel 2, the investigator can "check out" the transmission spectrum between 54 and 88 megacycles by moving progressively—and fine tuning 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 "scanning" the area with the rabbit ears at each frequency setting to cover up to 890 megacycle transmissions. Although this is an unlikely range for most of today's modern surveillance equipment, the state of the art is rapidly developing and, in the countermeasures business, no possibility must be overlooked. Also, these high frequencies may provide the investigator with a simple method of picking up a harmonic of a much lower frequency.

There is one possible drawback to this seemingly simple procedure. If the eavesdropper is using a transmitter triggered on or off by a remote control and has reason to believe counter-surveillance is being used, he can simply turn off his bug and there 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 costly. An experienced investigator may however, after reasonably 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.

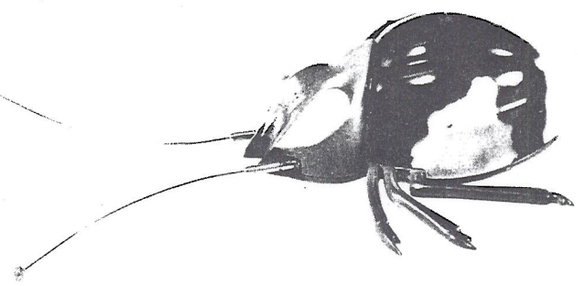
For greater security, even after a room has been searched, business firms holding top priority conferences should make some provisions during such conferences for the use of background music or some jamming device as a neon transformer.

The problem with jamming devices is that they will not interfere with wired microphones and may interfere with legitimate FM broadcast transmission, bringing down the wrath of the Federal Communications Commision.

**********

Telephone taps are often used in connection with tape recorders which begin operating when the phone is lifted off the hook or people begin to speak over the line.

When a telephone tap is suspected, one of the most effective defensive moves is to dial the recorded time signal. Once the signal begins, the voice-activiated bug will begin transmitting. If the unit is battery powered, the longer the time signal is permitted to repeat its mindless course throughout the day, the lower the battery of the bug will run.



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

If the device is running off telephone or house current, this procedure will, at least, be very aggravating to the eavesdropper.

Another defensive technique is to remove the handset from the 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 automatically 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 strength meter, as previously described, can detect a wireless phone tap by picking up the recorded time signal when this is dialed.

Each separate telephone system should be checked with a radio frequency bug detector, with the handset both on and off the hook. Breaks in the line suggest that a tapper has been at work, though with the increased use of the induction coil, no tell-tale bared wires are left behind.

One of the simplest, least expensive and most effective methods of checking for so-called "hot-mike" installations on telephone and intercom systems is by obtaining a particular kind of induction coil called a "Snooper" from a police or detective quipment supplier such as the one described above.

The most basic visual methods of checking a phone line for a tap 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 screws and terminals for scratch marks which could suggest the use of alligator 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 induction unit and be hidden on top of the pole.

Another defensive method gaining favor is that of using phone scramblers which convert telephone conversations into sounds unintelligible to anyone not having a similarly frequency matched scrambling unit. Several companies specialize in the sale of this type instrument—which is battery powered and portable.

Once it is suspected that a phone is bugged or tapped, a physical search of the instrument should be made, preferably by someone familiar with telephone circuitry for extra wires and the hard-to-detect substitute mouthpiece. 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 jamming device has been placed 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 eavesdropper. 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 from 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 pipe (hence the name). The sound of the note generates a current which will activate the telephone. The phone will not ring; the handset while still in place on the cradle acts as a sensitive microphone and transmits over the phone line all conversations taking place in the room. This little goody used to be sold in California for $395.00.

**********

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

1. Discrete dissociation with those persons; 2. Direct confrontation with the eavesdroppers; 3. Consultation with a law enforcement agency; or, 4. Employment 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 either optimistic or pessimistic; it's just important that people know as much as they can and not give up. The right to a private, self-fulfilling life is still the goal and even becomes clarified in the face of the enemy ...