You may think your conversation is private but

There appears to be little control in Britain over the manufacture and sale of bugging devices. ETI has been investigating the current situation.

IT WILL COME as a big surprise to most readers that bugging is not in itself a criminal offence. Plant an RF bug in an office during working hours, listen in on highly confidential discussions and the worst that you II be got for - if you're caught - is operating a transmitter without a licence. Technically you could also be had for listening to 'an unauthorised transmission' but we know of no such prosecutions.

• Tep secret, illustrated siport citatorus de-tails 20 ready built security devices, automatic surveillance receiver, ben microphone, mini-radio-mics, telephone operated devices (infinity-harmonics etc.), electronic stethoscopes and many more.

The Younger Committee on Privacy which reported in 1972 quite rightly recommended that bugging in any form should be an offence, in itself, but it has not yet been acted upon. •

How serious is bugging?

In researching this feature we found ourselves continually coming up against stony silence - few people are prepared to discuss the subject and none would agree to having their comments personally attributed. Try



ELECTRONICS TODAY INTERNATIONAL - JANUARY 1978

to talk to a company that's advertising bugs and ten-to-one he'll tell you he's now stopped, but he will supply you. with equipment to 'sweep' your office (the technical term for finding other people's bugs).

It is possible to get some idea of the scale of things however. There are about ten companies in Britain openlyadvertising bugs - most of them appear to be very small. Even so this indicates that sales are unlikely to be worth less than £100,000 a year and since bugs are cheap, literally thousands are sold every year.

Most technical publications (this includes ETI) refuse to accept advertisements for these devices on the grounds that they are undesirable, not because we are not allowed to.

Where are these bugs used then? We suspect that the overwhelming number are bought as toys and not for any devious purpose but this still leaves probably several hundred that are bought for their stated purpose: of listening in on other people's business.

UNSCRAMBLER SUPER SALE: Our famous Code-Breaker works with all scanners and tunes all scramble frequencies only series COD's (501) minimum Mall orders to:

The vast majority of businesses are operated decently and honestly but in every sphere it is very useful to know

TO VICTIMS TELEPHONE



Arrangement of an infinity transmitter used to eavesdrop on sounds in a room thousands of miles away using the telephone as the microphone.

Exploded view of the US Great Seal presented to the American Embassy in Moscow in 1945. This ingenious device was passive in operation and could not be detected by most of today's anti-bugging equipment. When you appreciate that this was devised 33 years ago it makes one wonder how sophisticated modern-day intelligence equipment must be.

about your competitor's business. There are several ways of finding this out, the commonest is to head-hunt a senior employee but his information is quickly out-of-date once he has left. Even knowing what's going on in R&D has serious limitations since even the staff in these departments don't know if their work will eventually get into production.

Bribery has been tried but you run. the very serious risk of meeting one of the 95% of employees who would report it to their boss.

Bugging is anonymous. Even if the bug is found, it's almost impossible to find out who planted it and since the

WALLS HAVE EARS



This telephone insert looks pretty standard. In fact it contains an FM radio transmitter with a range of several hundred metres.

risks to a company initiating bugging are enormous, middlemen are almost always used.

Superbur, noi just another bug, high stability FM transmitter, with 20 mile range, man, Minibur, tinier than exactbor, 5 miles range, for use, best value available, sae for details.

Sweeping

Many, if not most of the companies selling bugs will also supply sweeping equipment — after all a radio signal is easier for someone close to the transmitter to pick up than it is for someone a hundred metres away — or is it? First you don't know what frequency it's operating on. It could in theory be from 50 kHz (though the antenna would be a problem) up to several hundred megahertz. OK, use an untuned circuit but then what do you do about regular radio and TV broadcasts? If you set the frequency of the bug close to that of a powerful FM station it's difficult to sort out the two.

The makers of the equipment are highly secretive about their techniques and not one would discuss technicalities; they claimed, perhaps with some justification, that if you know how the sweeping is done, its all the easier to use a technique which won't be picked up. We believe many of them employ a howl-round technique — put a receiver near a bug and you'll set up an audio/RF loop which will go into oscillation.

Micro transmitters, receivers, electronic stethoscopes, etc., complete range of professional evilapment available, send 64,07 stamp for fully illustrated catalogue, local agents in many arcas.

International Espionage

Although companies will normally keep quiet about attempts to bug them, Governments delight in exposing the failed attempts.

The American Embassy in Moscow recently announced that they were being subjected to extremely high



A small bug openly advertised in Britain. Claimed to have a range of 200 metres with a 50-hour battery life, it retails for under £40.



The size of this bug can be judged from the PP3battery plug. It is claimed to have an output of 300 mW which the makers claim is good for 5 miles and can be supplied with any frequency in the range 84-150 MHz. We have no way of verifying these claims; price is about £16.

power, high frequency radio signals. It was of such a magnitude that it was even suggested that it was an attempt deliberately to make the staff ill. It is now thought far more likely that the RF signals were being used to recharge batteries in bugs within the building.

In 1945, as a gesture of good will, the Russians presented the US Embassy in Moscow with a beautiful wooden carving of the US Great Seal. After several years it was discovered that that this had built into it a wonderfully simple bug. Inside the seal was a copper cavity coupled to an antenna; one end of the cavity was covered by a thin metal diaphragm.

The bug was activated by an external RF signal (in fact 330 MHz) this made the cavity resonate but the diaphragm caused the reradiated signal to be modulated and this to relay conversations near the Seal. This could still have been in operation

DISSECTING A BUG

THE RF BUG shown in the photograph is a home-brew one that came into ETI's possession. The circuit was openly published in a British book a few years ago — we show the circuit as well although we have not, nor will we, provide any component values. (Since there are several variables we do not suggest you 'suck-it-and-see'.)

Although a DIY circuit, it would seem that virtually all the smaller or simpler bugs are of similar complexity or even similar circuitry.

This bug operates anywhere in the 87 MHz-108 MHz range and despite the simplicity and low battery drain (only a few milliamps) it will transmit a fair quality signal for several hundred metres in most areas and at least 30 metres even in heavily built-up areas

42

with steel-frame buildings like city centres.

The microphone will pick up normal speech at 10 metres quite easily. The performance, frankly, is worrying — because of the effectiveness — and the unit can be built for about £3!



Complete circuit of a VHF bug which can be built for only a few pounds.

ELECTRONICS TODAY INTERNATIONAL - JANUARY 1978

if some British technicians had not stumbled across the signal by accident. A thorough subsequent 'sweep' of the US Embassy brought to light no less than 60 other devices It is hardly surprising that British

Intelligence Services are involved as well. The Russian Embassy in London moved a year or so ago and when access to the building became possible it could be seen the lengths to which the Russians went to prevent eavesdropping, even to having built a room within a room. Various bits of information have leaked out that Intelligence Services were directing a low power laser at the window glass; this would then have been slightly modulated by the sound inside the room and the reflection picked up could detect this.



One of the techniques which has recently come to light is that of 'RF flooding' of a telephone. Even when the phone is on the hook, the RF can 'jump' the contacts. This is then modulated by the microphone and can be picked up. As it can only be used with single lines, a switch-board defeats this technique.

The other phone tapping technique, the 'infinity transmitter' is also made useless with a switchboard. Many company executives use direct lines for security whereas the switch-board itself is a pretty good defence against some techniques.

Tramistarised transmitters (not licensable in! UX), eutstanding raiue, easy-build kits include microphone, FCB and all electronic components, all VHF/FM tunable 70-160 mbz FM4 30275mm 400 yards, OUT FM100, S0175mm 3 miles, 1,200 yards, Super FM100, S0175mm 3 miles, ather kits arailable, including test gear, yoice switches and entertainment audio, send two or sac for detailed price list to:

Equipment Available

Laws in many countries have failed to keep pace with technology but it is ironic that most of the really sophisticated equipment being made originates in the US — the very place

ELECTRONICS TODAY INTERNATIONAL -- JANUARY 1978

and a supervision of the supervi

BEING BUGGED?

ARE YOU

THE BIGGEST PROBLEM facing someone wishing to bug another is gaining access, Breaking and entering is obviously criminal but a bug can be installed literally in one minute if some risk of the device being discovered is acceptable. Unless the villains have access to a building during building or decorating work, problems in slting the bug are real — well-concealed hiding places are usually bad for picking up sound. Favourite sites reported to us are in low pressure air-conditioning vents and behind radiators — another one is on sticky 'pads under a desk, somewhere which would not be noticed for years. A simple search is best and most bugs

A simple search is best and most bugs will be discovered unless a true expert has been employed.

The extent of telephone bugging is unlikely to be high — access is so difficult that only the Intelligence services will be able to handle this. In any case electronic telephone scramblers can overcome this. If you regard yourself as a candidate for bugging, check the credentials of Post Office engineers if you haven't called them in yourself. But don't be fooled by the novelists who seem to insist that 'two ominous clicks' after the telephone is lifted is a certain indication that there is an unwanted listener on the line.

with the strictest laws against bugging and phone tapping. This could be because the problem there is greater but no amount of legislation is going to prevent the availability of equipment — the profits are too great.

UNSCRAMBLE CODED MESSAGES from Police, Fire and Medical Channels. Same day service, Satisfaction guaranteed.

The range of equipment is so varied and the interest so keen that in the Spring of 1977 a full scale exhibition of both bugging and antibugging devices was held in West Germany — a country which

At first sight an ordinary pen but look closer. Despite its size it has everything incorporated and will put out a signal over 100 metres for three days on one set of batteries.

S11. 18

1.34



A real spy kit advertised for 'the professional'. A 6-channel transmitter operating on VHF or short wave is supplied — there is a matching receiver. Also included is a cassette recorder mains operation facilities.

incidentally bans sales . . . except if it is marked as 'Export Only'. It's surprising how many retail outlets regard themselves in this field!

The Future

However superior anti-bugging equipment becomes, the number of ways of eaves dropping electronically is so varied and the techniques developed for keeping the devices undiscovered so ingenious, it seems that bugs and bugging are not likely to become any less of a problem.

Legislation may not stop bugging but it can raise the risk factor to such a level that those practising it will think carefully.



ETI is not prepared to answer any queries, for whatever reason, on the circuit components or as to the availability of the equipmentshown in this feature.

43

Welcome to the world of "forbidden" information. This brochure will introduce you to our very special line of reading materials, but these are just two of many more, fascinating, hard-to-find books on unusual subjects, (CIA training manuals included), listed in our illustrated, 24-page catalog--

المناجع بمعارضة المحار

We sell the books you've heard about but can't find in bookstores because of their controversial nature. Unlike most book sources, we practice the principles of The Constitution by NOT deciding what you should read. If you are old enough to vote and be drafted, YOU decide that! Our business is unusual information and we are at the service of the Free American citizen. You will find that our product line includes the best books, manuals and reports available on the subjects of:

ELECTRONIC SURVEILLANCE SECURITY POISONS SURVIVAL SPECIALIZED ELECTRONICS INVESTIGATIONS LOCKSMITHING & LOCK TECHNOLOGY EXPLOSIVES and DEMOLITIONS FIREARMS AND SILENCERS HOME-MADE DEFENSIVE WEAPONS "STREETWISE" SURVIVAL SKILLS THE COVERT SCIENCES

If you tend to be timid or narrow-minded our materials possibly will offend your sensitivities, therefore we do not solicit your patronage. But if you are one who appreciates the uncommon, enjoys learning about the real world of intelligence, covert and undercover activities, crime and intrigue, you'll be glad you found us. Your privacy is assured and your satisfaction with our products is guaranteed.

There are two ways to get The INTELLIGENCE LIBRARY: Order it separately and pay two dollars, (to cover our cost and First Class mailing), or order one, (or both), of the two, excellent titles described in this brochure and The INTELLIGENCE LIBRARY will be included with your order.

So, if you want to break away from the world of dull, routine reading, just fill out the coupon below and get ready for reality!

ENTOR PUBLICATIONS 35-53 Northern Boulevard	
lushing, New York 11354	Date:
Send the items checked below:	
The ILLUSTRATED ART OF LOCK PICKING	\$7.95**
ELECTRONIC SPYING	\$7.95**
The INTELLIGENCE LIBRARY, (only)	\$2.00, (postpaid)
* Add 75¢ per book for Fourth Class postage,	or \$1.50 per book for First Class
NAME	
ADDRESS	
CITY	
STATE	ZIP-

• WIRELESS TRANSMITTERS, (radio bugging devices.)

S "BUGGED" APPLIANCES, (lamps, ashtrays, etc.)

✤ HOW BUGGING DEVICES ARE INSTALLED -- and where.

• WIRED MICROPHONE BUGS, (extremely common.)

HOW AN ORDINARY TELEPHONE IS USED TO BUG A ROOM.

The notorious "INFINITY TRANSMITTER." An ingenious device which enables an eavesdropper to listen to the slightest sounds in any room where a tiny device is concealed, simply by dialing the telephone number from any other telephone and sending a special tone over the lines.

BUGGING BY VOICE-CONTROLLED TAPE RECORDER. (Voice-controlled tape recorders are now legally available!)

LISTENING THROUGH WALLS, (the "spike-mike," etc.)

"ON-PREMISES" and "OFF-PREMISES" TELEPHONE TAPS.

TELEPHONE WIRING, (an education in itself.)

RECORDING TELEPHONE CONVERSATION, (now legal in many areas.)

TRANSMITTING TELEPHONE CONVERSATION TO AN ORDINARY FM RADIO.

BARGAIN BASEMENT" WIRETAPPING AND BUGGING BY SUSPICIOUS SPOUSES, (or, pre-divorce "dirty tricks," an extremely common activity.)

THE AMATEUR SPY.

...and more.

This easy to understand book provides more information than is available from many, six-hour security seminars costing hundreds of dollars. It is not a technical book, but it does a fine job of explaining an otherwise complicated subject, in ordinary, down-to-earth terms.

If you are one of those who hears about electronic surveillance and wonders how it is done, **ELECTRONIC SPAINC** is the book you've been looking for!





As the disturbing realities of Big Brother technology become more and more apparent, through an increasing number of news reports of wiretapping and other forms of electronic surveillance, even the most ordinary citizen is beginning to wonder if it is "safe" to talk on the telephone and if his or her most intimate, private conversations and actions are secure from deliberate eavesdropping. The truth is the ordinary citizen would be astounded to know how easy it is for anyone with a little motivation and simple know-how to listen to and/or make tape recordings of the private conversations and activities of others.

Electronic surveillance once was a secretive, mysterious, "dark science," which was practiced only by extremely knowledgeable technicians and specially-trained intelligence operatives, but this is no longer true. Because of the phenomenal growth and development of electronics technology it is now possible for anyone with the slightest motivation to tap a phone line, or bug a room, with the aid of a wide variety of inexpensive, readily-obtainable gadgets-- most of which are purchased openly from electronics dealers or by mail-order. This is an era of amateur spying, in which countless thousands of corporate boardrooms, ordinary bedrooms, "private" offices and telephone lines are being efficiently monitored, both by professional operatives and novices alike, some of whom barely understand how a flashlight works!

CALCULATE STATULE is the non-technical reader's most fluent source of information on this sensitive, secretive subject. It describes a wide variety of devices and how they are used, dispelling the myths and clarifying the realities of the very real threat of privacy invasion. This is a no-nonsense, "nuts & bolts" material, written in plain language by an experienced counter-surveillance specialist. It contains many photographs and illustrations, but no complicated schematics or theoretical text.

Unlike other, "suggestive" materials on the subject this book is quite explicit, showing exactly how bugs and wiretaps work-- and how they are used by amateurs as well as expert spies. One chapter is devoted to a very simplified explanation of telephone wiring, leaving no question as to how vulnerable it is to tapping, exactly how it is done, and the incredibly simple devices used to do it.

This material is unusually graphic, therefore the reader is warned that any form of electronic surveillance, even the secret tapping of one's own telephone lines or the bugging of one's own home, is illegal. This book is offered for informational purposes only, with the objective of defensive security in mind. Actual use of the information it contains would be unlawful, except in the process of courtauthorized investigations.

The following page contains a listing of some of the subjects covered:



This book is the single, most authoritative source of information available on the highly secretive subject of lock-picking. It has become a widely recognized, valuable educational reference for thousands of student and apprentice locksmiths. It was selected as the textbook for an accredited trade school course, it has been a long-time favorite of many investigative, security and law-enforcement professionals, and it is used in the training of the most sophisticated intelligence operatives in Government service.

It is a fact that more than 90% of the locking devices currently used in America, (the conventional "pin-tumbler" type), are extremely vulnerable to picking because of an inherent flaw in their basic design! This fact is commonly known to the lock manufacturing industry and all professional locksmiths. Only the consumer, the user of these relatively insecure devices, has been kept totally un-informed of this important, commercial "secret."

Opening these devices without a key is in many cases a fairly simple procedure, often possible within a few seconds, for anyone who understands the "secret" flaw in their ingenious, but fallible mechanism: This excellent book clearly reveals that secret and describes the classic techniques of lockpicking in exhaustive detail, in plain language, through easily comprehensible explanations which are amply supported by many illustrations and photos.

In addition, the illustrated art of EOCK PICKING contains separate, step-by-step lessons on disassembly and reassembly of the pin-tumbler cylinder, a simple, but foolproof method of developing expert skill at lock-picking, and full descriptions of the clever, mechanical devices sometimes used for the purpose, including the pick-gun, vibrator picks, the "snapper," etc. Finally there is a fully illustrated description and explanation of the rapid method of opening these cylinders by drilling the core with a cordless power drill. (This book describes the right way of doing it.)

We unconditionally guarantee this to be the most informative book of its kind in existence and a remarkable value at the low price. There is no trade or correspondence course that teaches more about lock-picking than this book does-- and some teach less. Countersurveillance

Never before has so much professional information on the art of detecting and eliminating electronic snooping devices—and how to defend against experienced information thieves—been placed in one VHS video. If you are a Fortune 500 CEO, an executive in any hi-tech industry, or a novice seeking entry into an honorable, rewarding field of work in countersurveillance, you must view this video presentation again and again.

ORDER LINE—1-800-522-6260

Wake up! You may be the victim of stolen words—precious ideas that would have made you very wealthy! Yes, professionals, even rank amateurs, may be listening to your most private conversations.

Wake up! If you are not the victim, then you are surrounded by countless victims who need your help if you know how to discover telephone taps, locate bugs, or "sweep" a room clean.

There is a thriving professional service steeped in high-tech techniques that you can become a part of! But first, you must know and understand Countersurveilance Technology. Your very first insight into this highly rewarding field is made possible by a video VHS presentation that you cannot view on broadcast television, satellite, or cable. It presents an informative program prepared by professionals in the field who know their industry, its techniques, kinks and loopholes. Men who can tell you more in 45 minutes in a straightforward, exclusive talk than was ever attempted before.

Foiling Information Thieves

Discover the targets professional snoopers seek out! The prey are stock brokers, arbitrage firms, manufacturers, high-tech companies, any competitive industry, or even small businnesses in the same community. The valuable information they filch may be marketing strategies, customer lists, product formulas, manufacturing techniques, even advertising plans. Information thieves eavesdrop on court decisions, bidding information, financial data. The list is unlimited in the mind of man—especially if he is a thief!

You know that the Russians secretly installed countless microphones in the concrete work of the American Embassy building in Moscow. They converted what was to be an embassy and private residence into the most sophisticated recording studio the world had ever known. The building had to be torn down in order to remove all the bugs.

Stolen Information

The open taps from where the information pours out may be from FAX's, computer communications, telephone calls, and everyday business meetings and lunchtime encounters. Businessmen need counselling on how to eliminate this information drain. Basic telephone use coupled with the user's understanding that someone may be listening or recording vital data and information greatly reduces the opportunity for others to purloin meaningful information.

The professional discussions seen on the TV screen in your home reveals how to detect and disable wiretaps, midget radio-frequency transmitters, and other bugs, plus when to use disinformation to confuse the unwanted listener, and the technique of voice scrambling telephone communications. In fact, do you know how to look for a bug, where to look for a bug, and what to do when you find it?

Bugs of a very small size are easy to build and they can be placed quickly in a matter of seconds, in any object or room. Today you may have used a telephone handset that was bugged. It probably contained three bugs. One was a phony bug to fool you into believing you found a bug and secured the telephone. The second bug placates the investigator when he finds the real thing! And the third bug is found only by the professional, who continued to search just in case there were more bugs.

The professional is not without his tools. Special equipment has been designed so that the professional can sweep a room so that he can detect voice-activated (VOX) and remote-activated bugs. Some of this equipment can be operated by novices, others require a trained countersurveillance professional. The professionals viewed on your television screen reveal information on the latest technological advances like laserbeam snoopers that are installed hundreds of feet away from the room they snoop on. The professionals disclose that computers yield information too easily.

This advertisement was not written by a countersurveillance professional, but by a beginner whose only experience came from viewing the video tape in the privacy of his home. After you review the video carefully and understand its contents, you have taken the first important step in either acquiring professional help with your surveillance problems, or you may very well consider a career as a countersurveillance professional.

The Dollars You Save

To obtain the information contained in the video VHS cassette, you would attend a professional seminar costing \$350-750 and possibly pay hundreds of dollars more if you had to travel to a distant city to attend. Now, for only \$49.95 (plus \$4.00 P&H) you can view *Countersurveillance Techniques* at home and take refresher views often. To obtain your copy, complete the coupon below.

RADIO-ELECTRONIC 500-B Bi-County Blvd, Farmingdale, NY 11735		OFFER	RE
Please rush my copy of the Video VHS Cassette for S handling.			
No. of Cassettes ordered Amount of payment \$			
Bill my VISA I Ma Card No Expire Date/	<u></u>		
Signature Name Address City		ZIP	
All payments in U.S.A. VHS cassette. No foreign add applicable sales tax.	funds. Can n orders. New	adians add \$4	.00 per

CALL TODAY TO ORDER 1-800-522-6260

NOVEMBER 1990

ner/soncarder delectors, voice scrampiers, unusual kits, CAPRI ELECTRONICS, Route 1R. Canon, GA 30520 THE Intelligence Library-Restricted technical information & books on electronic surveillance, surveillance-device schematics, lock-picking, investigation, weapons, identification documents, covert sciences, etc. The best selection available. Free brochures. MENTOR. (Dept. Z). 135-53 No. Blvd., Flushing; NY 11354. WHOLESALE MATV/CATV equipments, antenna, accessories, cartridges, radios, speakers, cables.

SINGAPORE-shopper's paradise. Get components, peripherals, books and equipment-very cheap. Send requirements, BUSINESS BIRDS. B1-47, Simlim Tower, Singapore-0820, . UNIQUE video countermeasure and counter-court termeasure manual. Limited distribution. Covers satellite, CATV, STV, MDS. Information, 1985 catalog, application notes \$1.00 plus 2 oz S.A.S.E.. CAPTAIN VIDEO, P.O. Box 9388, Baltimore, MD 21228. d, 1. FLY'S .#1 to #692, yokes, modules, much more Send-stamps, 55 cents to WHOLESALE ELEC.