iPROTECT 1210

Portable bug detector

USER MANUAL

Introduction

Thank you for purchasing the iProtect 1210 countersurveillance indicator. This card-sized device belongs to a new generation of personal sweeping equipment. It can be carried in a pocket or wallet and not attract the attention of other people. When it is necessary, it will easily and quickly help you check for the presence of bugging devices in any given area.

About bugging

According to the 'Granite Island Group', an internationally recognized leader in the field of Technical Surveillance Counter Measures (TSCM), (Bug Sweeps, Wiretap Detection, etc.,) the manufacture, sale, installation, and monitoring of illegal surveillance devices is a multi billion underground industry. It is reported that in the United States over six millions dollars worth of surveillance devices are sold to the public each day. Most of these products are sold from storefront operations, spy shops, attorneys, and via private investigators located in major metro areas such as New York, Miami, Los Angles, San Francisco, Dallas, Chicago, and Minneapolis.

This does not include the tens of billions spent each year for legitimate eavesdropping products purchasedby law enforcement, military, and intelligence agencies.

The majority of this equipment is illegally imported from France, Germany, Lebanon, Italy, Canada, Israeli, England, Japan, Taiwan, South Africa, and a host of other countries. Additionally, anyone with a soldering iron and a basic understanding of electronics can build and install an eavesdropping device.

The raw materials to build such a device may be easily obtained at a components supplier or salvaged from consumer electronic devices such as cordless telephones, intercomsystems, and televisions.

This equipment is commonly sold over the counter, via mail order, and through the Internet. Most of these bugging devices cost only a few dollars, but highly sophisticated, quality products may be purchased for less than one thousand dollars. In New York City alone there are over 85 companies which will not only sell you the eavesdropping device, but will break into the targets office to install the device, and for an additional fee will provide a monitoring and transcription service.

The FBI and other federal law enforcement agencies have repeatedly indicated that they lack the resources and training to enforce or properly investigate the technical security threat within the United States.

Signs of bugging

According to the Granite Island Group, these are the following signs of covert eavesdropping or bugging:

- others know your activities, confidential business or professional trade secrets
- secret meetings and bids seem to be less than secret
- You have noticed strange sounds, static, popping, scratching or volume changes on your phone lines.
- Sounds come from your phone's handset when it's hung up.
- Your phone often rings and nobody is there, or a very faint tone, or high pitched squeal/beep is heard for a fraction of a second
- You can hear a tone on your line when your phone is on the hook (by using an external amplifier).
- Your AM/FM radio or car radio has suddenly developed strange interference
- Your television has suddenly developed strange interference.

- You have been the victim of a burglary, but nothing was taken
- Electrical wall plates appear to have been moved slightly or "jarred"
- A dime-sized discoloration has suddenly appeared on the wall or ceiling
- One of your vendors just gave you any type of electronic device such as a desk radio, alarm clock, lamp, small TV, boom box, CD player, and so on.
- The smoke detector, clock, lamp, or exit sign in your office or home looks slightly crooked, has a small hole in the surface, or has a quasi reflective surface
- Certain types of items have "just appeared" in your office or home, but nobody seems to know how they got there
- White dry-wall dust or debris is noticed on the floor next to the wall
- You notice small pieces of ceiling tiles, or "grit" on the floor, or on the surface area of your desk
- You notice that "Phone Company" trucks and utilities workers are spending a lot of time near your home or office doing repair work.
- Telephone, cable, plumbing, or air conditioning repair people show up to do work when no one called them
- Service or delivery trucks are often parked nearby with nobody (you can see) in them
- Furniture has been moved slightly, and no one knows why
- Things "seem" to have been rummaged through, but nothing is missing (at least not that you noticed)

What are bugging devices?

A "Bug" is a device which is placed in an area which then intercepts communications and transmits or conducts them out of that area to a listening post. The eavesdropper can be just a few feet away from the victim, hundreds of feet, or even miles depending on the kind of bug used. There are five primary categories of "Bugs": acoustic, ultrasonic, RF, optical, and hybrid. An RF (or Radio Frequency) Bug is the most well known type of bugging device. A radio transmitter is placed in an area or in a device. It is extremely easy to detect, but cheap, disposable, anddifficult to trace back to the person who planted it.

Unfortunately there is no magic 'black box' which detects all the bugging devices quickly and simultaneously. Each category needs certain equipment and procedures to be detected and found. Protect 1210 can help in searching for RF devices. According to the way of broadcasting, they can be divided as follows:

- Common VHF/UHF transmitters
- Video transmitters
- Digital transmitters with continuous carrier
- Digital transmitters with storage, compression and short-time transmission
- Spread-spectrum transmitters
- Hopping transmitters (frequently changing frequency)
- Transmitters using standard communication protocols (for example, GSM or DECT transmitters).

According to the sort of transmitted information RF bugging devices can be divided into the following types

- room or body-carried transmitters
- telephone line transmitters
- universal room/phone line transmitters, transmitting both room acoustics and phone conversations
- vehicle tracking devices

Features

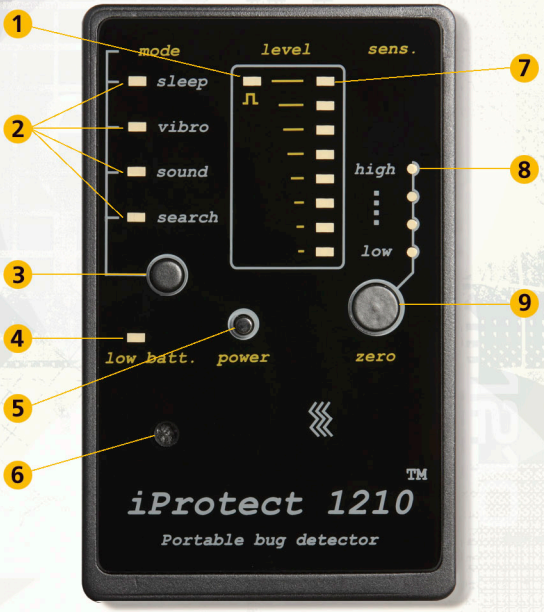
The countersurveillance indicator iProtect 1210 has been designed for solving the following tasks:

- Searching for active radio transmitting surveillance devices (or RF bugging devices) in premises, vehicles and items
- Discovering the improper use of mobile phones and other communication equipment for picking up conversations.
- The information in this case can be transmitted to another phone or recorded onto an answering machine.
- Detection of harmful emissions from GSM-jammers or mini recorder suppressors
- Detection of harmful emissions from microwave ovens, communication antennas and other electronic appliances

Main features of the iProtect 1210

- Detection of all kinds of active radiotransmitting devices including digital signals
- Operation driven by microcontroller
- Card-style durable body. Does not attract people's attention when used or transported.
- Working frequency range 50-3000 MHz
- 4 working modes: Normal, Sound, Vibro and Sleep
- 8-segment bargraph indicator for precise measuring of the radio field level and location of a bugging device
- Integrated antenna
- Calibrated sensitivity for rejection of background fields
- “Low battery” indicatior
- “Pulse” indicator for recognizing digital transmitters including GSM and DECT
- Powered by a CR2430 lithium battery

Parts and controls



1 'Pulse' indicator
This LED lights up when a pulse field is present near the unit. Such a field is usually produced by GSM/DECT telephones or can be created by a bugging device with a 'non-standard' type of transmission.

2 Indicators of working mode

3 Button for selection of working mode:

- **Normal**. In this mode the iProtect 1210 will indicate an increase of the RF level on the bargraph. No sound will be produced.
- **Sound**. In this mode the iProtect 1210 will produce the sound of a demodulated signal. In close vicinity of the FM-modulated bugging device a loopback effect should appear. A buzzing sound will appear near digital transmitters like an active GSM phone. This mode allows the user to identify the transmitter.
- **Vibro**. This mode is used for covert operation or for situations when the operator cannot watch the bargraph. An increase of the RF level will cause the built-in vibrator to activate.
- **Sleep.** In this mode the iProtect 1210 wakes up every 3 seconds and checks the current RF environment. If there is an increased level the unit will indicate this with an alarm sound. The detector will stay active until the high level disappears.

4 This indicator turns on when the battery is low and should be replaced

5 Power on/off

6 Speaker

7 Bargraph indicator. Displays current level of the electro-magnetic field and helps the user to locate bugging devices. Location is carried out by moving the unit into the strongest level area. The bargraph consists of 8 LEDs and shows the current level with the help of 3 of them at any one time. As the field becomes stronger this group scrolls up. For powerful signals the group goes up further until two or one diode remains on.

8 Indicator of the current sensitivity level

9 Zeroing the sensitivity of the detector according to the current RF level. The unit will store the current level and clear the bargraph so that it will show stronger signals only. Perform this action before approaching the target zone or when you are trying to locate the RF source. Use this control each time it is necessary to re-tune the sensitivity — when you enter an area with a lower or higher level of background noise.

Antenna

The antenna of the unit is situated on the rear side under the 'iProtect 1210' label. It receives electro-magnetic waves and passes them to the unit's circuit board. It is necessary to direct this side of the detector towards probed items and surfaces when performing a search.

Usage

Sweeping the room

Before starting sweeping, you should carry out some preparation tasks. Firstly, it is necessary to consider the time of the sweep and the situation. Since there are lots of devices that are remotely controlled, it is recommended to carry out a sweep during working hours in real situations when the eavesdropper most wants to listen. It may be necessary to arrange a fictitious meeting. Nobody has to know about the pending search.

Close all drapes in the room. Turn on all the lights and activate any other devices to imitate normal conditions. It is also advisable to turn on a source of sound such as a stereo system or radio. This sound source has two very important functions:

- Voice activated transmitters will be activated
- Your actions will be masked

1. Leave the room, turn on your iProtect 1210 and adjust its sensitivity by pressing the 'ZERO' button. Before adjusting the sensitivity make sure that there are no working radio transmitters in the close proximity to the unit (1-5 meters) — GSM or radiotelephones, radio transceivers, etc. Otherwise you may set the sensitivity to an excessively low level.

2. Choose the operation mode. For covert procedure use the Normal or Vibro mode. The Normal mode is more convenient for locating the RF source. The Vibro mode allows the operator to avoid constantly watching the bargraph when inspecting areas that are difficult to access. The Sound mode allows the operator to listen to the signal so that he or she can understand more about the source.
Note: a loopback effect may appear near an active bugging device in this mode. It is obviously a clear sign of danger for you, but may also allow an eavesdropper to discover your counter surveillence operation.

3. Enter the room holding the iProtect 1210 and watch its bargraph or pay attention to the vibrator. Turn the lights and other equipment in the room on and off. Walk around the room while watching the indicatiors or feeling for the iProtect's vibration. The bargraph level, or the frequency of impulses, will increase or decrease when the detector is closer to or farther from a transmitting device.
Probe all objects which may contain a hidden surveillance device. When you get close to an RF bugging device the bargraph of your iProtect 1210 will rise (or vibration will appear). The distance of detection may vary depending on the situation. Usually the iProtect 1210 will detect an average radio microphone at a distance of 20-60 cm although it is recommended to probe the objects at a proximity of 10 cm. The bargraph can display 10 different levels. The lowest level is shown by the first LED. As the RF level grows, a group of three diodes will scroll up on the bargraph until only the one 'upper' LED will remain; in the case where a very high level signal is detected.

You can use the 'ZERO' button to decrease the sensitivity gradually when performing the location procedure (finding the source of the RF field). Press this button when the bargraph shows a high level to force the unit to react to a stronger field only. Thus you will find the place with the strongest field.

Please note: if you want to continue sweeping after the location of one bugging device, it is necessary to restore the normal sensitivity of the iProtect 1210. Press the 'ZERO' button after making sure that the detected transmitter does not affect the unit (It is turned off or is at a sufficient distance away). If you want to restore the maximum sensitivity turn off the iProtect 1210 and then turn it on again.

The bargraph may often show an increased level near wires or metal objects. This may not be a bug, but rather the metal acting as an antenna extension. A similar situation may appear in the apertures of windows due to radio waves coming from the outside. In these situations you can decrease the sensitivity by pressing the 'ZERO' button.

4. After you have found the exact location of a high field, try the Sound mode if secrecy is not critical. A Loopback effect will clearly confirm the danger. Not depending on the presence of a loopback, start a physical search.
Visually inspect and probe each object in the highlighted area. Disassemble, if necessary, lamps, desktop items, telephones, AC outlets, phone outlets. Inspect all power and phone lines carefully. Open books, wardrobes, etc.
Remember, that a physical search is a fundamental operation during the sweep.

If you find a bugging device, do not stop! You should continue the search more carefully as eavesdroppers often install more than one device. They may install a so called 'foolish bug' which may be easily detected and some other well hidden devices that may have remote control and non-standard modulation.

5. In the modern environment mobile phones are very often used as bugging devices. Therefore if the unit's “Pulse” indicator starts to light, suspend the search and wait for a while. It could be a signal from a working telephone in a neighboring flat or office. Use the Sound mode to listen to the signal. The GSM signal will have typical 'buzzing' sound.

Checking telephone lines

Telephone bugs may be installed anywhere a phone line lays. It may be within the phone set, the phone outlet, connecting box or cable. Most telephone bugs activate only when the receiver is off-the-hook. Therefore the sweeping of phone lines should be carried out only when the receiver is in this state.

Start checking from the phone set. Place the iProtect 1210 near the set and lift the receiver. Watch for an increase of the RF level (or starting of the vibration). Please note: It is pointless to test wireless (radio) telephones, for they act exactly like a bugging device themselves due to the use of radio waves. Only a physical inspection of these items is sufficient to know if they are bugged.

Move the detector along the phone line while keeping it off-the-hook. Check all the outlets and communication boxes. If possible ask a second person to lift the receiver and then hang it up repeatedly. If you see that the RF level changes when the line is activated and deactivated, this is a sign of a bug's presence. Try to locate the place where the RF level is highest and then perform a physical search.

Working in the Sleep mode

In this mode the iProtect 1210 wakes up every 3 seconds and checks the current RF environment. If there is an increased level the unit will indicate this with an alarm sound. The detector will stay active until the high level disappears.

Testing people

There are many types of body-carried transmitters. They may broadcast conversations and (or) video signals.

Adjust the sensitivity to the current background level using the 'ZERO' button. While carrying the iProtect 1210, approach the person. If the level grows, it means that the person is carrying a transmitting device. If you have changed the location re-adjust the sensitivity by pressing the 'ZERO' button again at some distance from the person.

Another way to test people is to place the iProtect 1210 on the desktop. In the Normal mode it will be necessary to watch the bargraph carefully when the person approaches the table and sits down. You can also use the Sleep mode. If the person is carrying an RF transmitter the iProtect 1210 will detect it and produce an alarm.

GSM and DECT detection

Improper use of a mobile telephone can be discovered with the help of iProtect 1210. In this case the “Pulse” indicator will be on while the bargraph fluctuates rapidly.

Other applications

If you cannot inspect a whole room, for example, in a restaurant or someone else's office, the iProtect 1210 can be used for checking the closest objects to you. In a restaurant it may be necessary to check the items on a table or the table itself, since they can contain a bugging device. The card-style design suits this opertion perfectly.

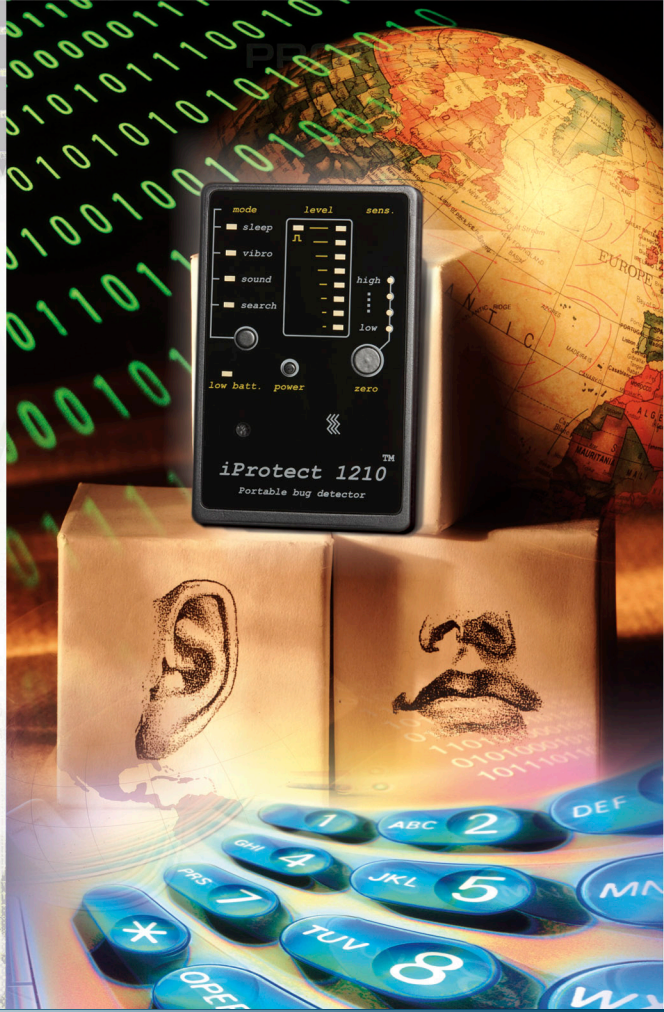
Detection distance

The detection range of the iProtect 1210 depends on two major factors:

- The output power of the bug
- The surrounding RF environment, such as radio/TV and communication devices

The level on the display of the iProtect 1210 will increase as you approach an RF source (or vibration will start). Either a surveillance transmitter or a safe signal (background noise) can cause it to increase. Successful location of a hidden bugging device is accomplished by finding the area which produces the highest level on the bargraph of the iProtect 1210. Normally, an active bugging device will be detected at a distance of 20-60 cm and a GSM telephone at 50-150 cm.

Specification	
Frequency response	50 - 3000 Mhz
Power supply	CR2430
Average current consumption	8.5 -16 mA (from 0.36 mA in Sleep)
Continuous operation	18-32 hours (50-90 hours in Sleep)
Dimentions	55x85x7 mm



SPY SHOP EUROPE.COM

Contact Us:
Tel. +385 51 673 400
Fax. +385 51 671 542

Mail:
info@spyshopeurope.com
sales@spyshopeurope.com

Beling d.o.o.
Franje Čandeka 23B
51000 Rijeka, Croatia
VAT No. HR 80249393012