



# ACTIVITY MONITORS

AKA: Cell Phone and Computer Eavesdroppers

This article is approved by the following for continuing education credit:  
The American College of Forensic Examiners International provides this continuing education credit for Diplomates.

After studying this article, participants should be better able to do the following:

1. Understand the various ways that eavesdropping can be accomplished by modern technology.
2. Guard against illegal eavesdropping.

KEY WORDS: key loggers, wiretaps, bugs, transmitters, Trojans

TARGET AUDIENCE: Security professionals

PROGRAM LEVEL: Basic

DISCLOSURE: The author has nothing to disclose.

PREREQUISITES: None

By Louis L. Akin, LPI

Thanks to the hefty law enforcement and civilian security budgets that drive the industry, eavesdropping technology has been booming for three decades, and invasions of privacy are easier to accomplish today than in any time in history. Cell phones can be turned on remotely to listen to live conversations, carrier current monitors can be attached to electrical house or office wiring to listen to what is being discussed inside, and keystroke loggers can be attached to or installed in computers to capture every password that is typed and every e-mail that is sent or even read. Small GPS locators can be placed on cars or motorcycles to monitor by remote computer every place the vehicle travels and record the exact address of each stop—and it's all done in real time. It's so easy to do that it's hard to resist doing it, legally or illegally. Who is going to know? This article is for law-abiding people who would like to learn some of the technology available and how it is utilized. Just because you're paranoid doesn't mean someone isn't eavesdropping on you.

An attorney and an expert witness are sitting in a café having coffee while on recess in a major case. They turn off their cell phones so no one will interrupt them, and both lean forward for a serious tête-à-tête about the expert's testimony. But they are not the only ones interested in their discussion—unknown to them, a third party miles away remotely turns on the attorney's cell phone and records every word of the conversation. When the conversation ends, the expert witness turns on his phone, calls his office, and gets the latest on what his assistant has developed on the case. The third party records that conversation too, and while she is at it, downloads all the text messages and e-mails the expert has on his cell phone. She also downloads the telephone numbers, dates, exact times, duration of the conversations, and the locations at which the expert was for every call that has been placed or received on his cell phone for the past month. Unbelievable? Not at all. It's happening.

Eavesdropping has been around as long as eaves, the beams that form the two long sides of an A-frame roof. Eavesdroppers supposedly used to climb to them to listen in on private conversations. Today, that kind of physical eavesdropping is no longer a credible threat. While it may be trespassing, or possibly burglary, the **Omnibus Crime and Safe Streets Act** (1968) doesn't prohibit it.

Technical surveillants, many of whom prefer to be addressed by the more Orwellian "**Activity Monitors**" appellation, have developed technical means of invading privacy. Common telephone taps are as old as the 1940s, but have grown progressively more sophisticated. The hook switch bypass was a device that circumvented the off button on the receiver of the old rotary dial telephones. In effect, the telephone microphone could be turned on remotely just as if it were off the hook and someone miles away could listen to what was being said in a room. In the 1950s, Manny Middleman devised a way to activate a hookswitch bypass by calling a telephone on which one was installed (which required a previous burglary to plant the hookswitch) and blowing a certain key on a harmonica into the phone. He could then listen to conversations for as long as he liked from wherever he liked.

Taps are devices that are placed on telephone lines for purposes of covert eavesdropping. Bugs are devices placed in a room

or area for the same purpose. Transmitters are physical objects that are easy to hide because of their incredibly small size, but they still require entry into the target area to plant (Electronic Surveillance Counterterrorism, 1989a). San Francisco private investigator Hal Lipset waltzed around a cocktail party in the 1960s with a transmitter hidden in an olive in his martini (Holt, 1993). The toothpick was hollowed out for the antennae. This was a considerable feat, considering he did it around the time when color televisions were beginning to appear in American homes.

**Eavesdropping devices** have kept abreast of the times, advancing from ultra-sophisticated electronics such as tiny frequency-hopping burst transmitters that compress and store conversations and then transmit them through the air in short bursts that hop about in a preset pattern amongst mul-

## **"Eavesdropping devices can be physically installed on cell phones or computers in a matter of seconds by an intruder"**



iple frequencies (Electronic Surveillance Counterterrorism, 1989b). To receive the messages, the eavesdropper has to know not only when they are going to be transmitted, but the exact order of frequency hops they will make during the short burst of transmission. The eavesdropper's receiver has to hop with the transmitter to capture the electronic bursts, then demodulate them.

Eavesdropping devices can be physically installed on cell phones or computers in a matter of seconds by an intruder (who may be a cleaning person, inspector, customer, witness, sales person, acquaintance, or burglar) or the device might be sent to the "target" by e-mail or text message. When programs are installed in the latter manner, they are called Trojans, a kind of virus that is packaged as something attractive or expected.

For instance, a consumer might get a text message on his cell phone saying "Call (314) 666-1234 to update your Verizon cell phone software," or "Download free new ring tones or screen savers." While these messages are usually genuine, they can be faked. When the consumer calls to get the fake update, he or she gets a Trojan that installs in the cell phone as a digital eavesdropping device. No burglary required. The phone will turn on so the eavesdropper can listen to conversations in the room or auto-dial the eavesdropper and give such private information as the telephone number, date and exact time of each call, and the location, within feet, of each incoming or outgoing call the cell phone owner makes or receives. It will also send any text messages or e-mail to the eavesdropper.

Vervata's \$49.95 FlexiSpy Pro tap ("Vervata" and "FlexiSpy Pro" are pseudonyms employed to describe an actual product) is one of the latest commercially available cell phone eavesdropping devices on the market, but it isn't the only one. Many competitors produce similar programs. Anti-virus software companies and tech writers condemn the program as blatant spyware that can turn on a cell phone (just like Manny Middleman used to do) and allow an eavesdropper to listen in on every conversation that takes place within earshot of the cell phone while the owner of the phone thinks it is off.

Vervata advertises its product as the "World's Most Powerful Spy Software for mobile phones. [FlexiSpy Pro] is a mobile phone monitoring application that secretly records all activity on a mobile phone

Advances in technology provide companies with more opportunities to connect with clients and the global market to boost their revenues and awareness. Unfortunately, such communications also create more holes in a company's security. Companies worldwide face these technological security threats. Web conferences are becoming more widely used for cost-effective, efficient communication with multiple sites. The downfall is the difficulty in keeping invite lists private and offering adequate security for lengthy conference meetings. With many video conferencing software programs, companies might not even realize they might have a side channel active on their server.

The security threats are even greater with using mobile devices like smart phones. As of last year, nearly half of Asian businesses used mobile devices to send and receive office e-mail, but most companies employed only 33% of the necessary security measures to keep the information confidential.

The Symantec group of Asia Pacific offers these tips for keeping corporate mobile devices safe:

**1. Put in place adequate protection measures**

Ensure that there are multiple layers of security such as a firewall or antivirus software and that they are able to run on different mobile platforms.

**2. Encrypt data**

Companies need to implement encryption technology to protect their mobile devices, especially if the users are entrusted with confidential information. This is to prevent important or sensitive data from being stolen.

**3. Administer network access control**

Identify access levels and classify users accordingly on a rigid basis to minimize the impact of data leakage.

Information from ZDNet, <http://www.zdnetasia.com/news/security/0,39044215,62052457,00.htm>

<b>Target Cell Phone</b> <sup>viii</sup>	➔	<b>FlexiSpy Pro Server</b>	➔	<b>Any designated computer</b>
<ul style="list-style-type: none"> <li>• SMS messages</li> <li>• E-mail</li> <li>• Telephone conversations</li> <li>• Live voice</li> <li>• Call history</li> </ul>		Holds for relay 24 hours a day 7 days a week		Any designated computer connected to the web may retrieve the information.

on which it is installed. Protect your children, catch cheating spouses—the possibilities are endless.” The possibilities for abuse are endless. According to the Vervata Web site, “You can listen in on calls and read SMS/MMS messages. What’s more, even when the phone is not in use, you can remotely activate the microphone and listen in on non-call conversations. Of course, the legality of this falls in a grey area.” Actually, it’s plainly illegal to use the tap on anyone but your minor children. Vervata adds the limp caveat on its Web site, “If you are the owner of your spouse’s (or child’s) cell phone, you are merely monitoring your property, but if you use FlexiSpy Pro on an unsuspecting neighbour, that’s a different story altogether.”

Vervata adamantly denies that FlexiSpy Pro is a Trojan, stating that it has to be consciously installed by a live human. Yet the critics disagree: “This application installs itself without any kind of indication as to what it is. And when it is installed on the phone it completely hides itself from the user,” says Jarno Niemela (2006), a researcher for F-Secure. This is a case in which both parties may be right—at least, on the surface. A person has to consciously install the program, but that person doesn’t have to be the cell phone owner. On the other hand, if it is sent as a Trojan, the person installing it may not know that it’s spyware. The missing words are, “effective legal consent of the cell phone user.”

Here’s how the FlexiSpy Pro model works when it is installed:

When FlexiSpy Pro.A is installed on the phone it will hide from Symbian’s built-in process menu and it does not have any visible user interface or icon. After FlexiSpy Pro.A is installed on the phone, the only indication that it is installed is that the application removal menu has an additional application named “phones” in the list. This “phones” application cannot be removed with the application manager.

FlexiSpy Pro.A has a hidden user interface that can only be accessed using a special code known to the person who has purchased the spying application and has installed it on the phone.

When FlexiSpy Pro.A is active on the device, it will record details of all voice call and SMS information, and then later send those details to the FlexiSpy Pro server. (Niemala, 2006)

Law enforcement has a more limited but more easily installed cell phone tap. Once they get your cell phone number, they go to a Web site to find your service provider. Then they obtain a search warrant, call the service provider, and have the provider clone the phone on which they want to eavesdrop. The provider overnights them a chip and thenceforth each time the target uses his or her cell phone to call out or receive calls or text messages, the police receive the calls and record them. No need to pull a burglary, no need to convince someone to use a Trojan, no chance of getting caught. This technique is an update of the lease-line method of tapping land lines that was popular before cell phones came along.

**Digital cell phone taps** may be the newest technology available to the general public, but plenty of the old gear is still around and it works well. FM radio frequency transmitters that sell for \$20 in electronics stores make ideal drop bugs, or disposables. Disposables are transmitter bugs that can be left somewhere to transmit until their battery runs dry, and they are then forgotten. The eavesdropper doesn’t have to make a second entry to recover the devices. These bugs are cheap and untraceable, and nearly every law enforcement agency uses them. So do private investigators, persons getting divorced, partners terminating a business relationship, possessive spouses, and others.

Carrier current devices are also available at electronics stores and are sold as baby monitor systems. Strip off the baby blue or pink plastic case and the device can be hidden anywhere in the house or building’s electrical system, inside or out. It will transmit conversations from inside the house or office along the AC wiring to a receiver down the line. Room-to-room plugs in intercom systems do the same thing and are used by eavesdroppers for the same purposes. They are also commonly available in electronics stores (National Commission, 1976). More sophisticated devices include light switches and wall plugs that really work to turn on the lights or run the vacuum, but they also work as transmitters when there is conversation in the room.

## Compromising Computers

Activity-monitoring software, also known as **key logger spyware**, has been in circulation amongst amateur and professional eavesdroppers, mainly law enforcement, for at least a decade or more. The FBI was the first agency to acknowledge using it. There are two versions of key logger eavesdropping devices. The first is a hardware device that attaches to the back of the computer and blends in with the other cables. Its disadvantage is that it requires a physical installation and has to be retrieved at some point. The other version of a key logger is software that can be sent by e-mail as a Trojan. It is the more insidious implant.

The key logger software programs sell in various stores for around \$100-200. The software is easily concealed in e-mail or as a Trojan, and it installs within seconds. Once installed, it gives erroneous file name information and changes its name and position each time the computer boots. Forensic computer analysts are needed to find, identify, and remove them and to make a forensic copy of the hard drive for purposes of evidence and testifying in court. Key loggers give a third party access to every file and document on the target computer's hard drive. Any strokes of the key will be replicated on the eavesdropper's computer screen. What the target says in e-mails, instant messaging, documents, spreadsheets, or anything else that comes up on screen will all be revealed to the eavesdropper. Equally as disturbing, the eavesdropper can learn all of the target's passwords, account numbers, and user names, including bank accounts and any credit cards the target uses online.

One key logger software manufacturer advertises this way:

WebWatcher is the most trusted name in Activity Monitoring Software, because we do what no one else can:

- Monitor in real-time from anywhere
- Block ANY webpage based on content or web address
- Read Instant Message (IM or "Chat") Conversations
- Read Incoming and Outgoing E-mail
- Log every keystroke
- Take screenshots
- Record online & offline activities
- Quickly sift through data using unique keyword system

You can watch over your target from anywhere. With WebWatcher's **web-based**

**monitor** you can check your recorded data from any computer in the world.

- Watch your target's activities in REAL-TIME
- See what your target is doing as they are doing it!
- Using our secure servers, your data is uploaded instantly, giving you the ability to react to situations before they become problems.
- It is completely invisible.

Designed to meet the exacting standards of intelligence agencies engaged in the war on terror, WebWatcher is completely invisible. Whether you are trying to monitor your computer savvy spouse or the head of your tech department, you won't be detected. WebWatcher doesn't appear in the Registry, the Process List, the System Tray, the Task Manager, on the Desktop, or in Add/Remove programs. There aren't even any visible files that can be detected (WebWatcher)!

Anyone who uses computers should heed these advertisements and keep in mind that the sales of spy equipment are of a magnitude sufficient to support an industry.

## Levels of Surveillance and Sweeps

There are four levels of technical surveillance and four levels of technical surveillance countermeasures. The level four "high tech" equipment used by the federal government may be so sophisticated that only the most advanced equipment can find it. On the other hand, federal and city law enforcement agencies are the biggest customers for disposable bugs and taps from electronics stores. So the fact that the federal or municipal governments are doing the eavesdropping does not necessarily mean they are using high tech equipment, but prudence would require a high tech sweep if they are suspected.

Mid-level technical activity-monitoring involves the use of good surveillance equipment and an eavesdropper who has a working knowledge of technical surveillance

technology and strategy. Low-level, or level one, eavesdropping includes phone taps and recorders hidden in homes or offices by amateurs. Though they can sometimes be found by accident, they can be easily missed by a person who is conducting a sweep but has not had training in countermeasures.

## Conclusion

Eavesdropping is probably more common today than any time in history. This article did not have room to cover the multitude of micro video cameras that fit inside the button of a shirt, a tie tack, the frame of an ordinary pair of eyeglasses, a wall clock, or baseball cap. And following a person can be done remotely by attaching a small GPS transmitter to his or her car and tracking via satellite. The technology is sophisticated and difficult to detect without using equally sophisticated search equipment. The toys are available to law enforcement as well the public at large.

We used to say: "Just because you are paranoid does not mean that someone is not following you." Now we can add: "... listening to every word you say and watching every word you type."

## References

- Electronic surveillance countermeasures. (1989a). Advanced course, Jarvis International Intelligence Academy. Tulsa, OK.
- Electronic surveillance countermeasures. (1989b). Advanced course, Texas A&M Extension Services.
- Holt, P. (1993). *The Bug in the Martini Olive*. Random House Value Publishing.
- Niemela, J. (2006, March 29). "First Trojan spy for Symbian phones." F-Secure Trojan Information Pages. Retrieved from <http://www.f-secure.com/weblog/archives/archive-032006.html>
- National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance. (1976). "Wiretapping and electronic surveillance." Washington DC: GPO.
- Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. § 3789d (1968).
- WebWatcher Computer Monitoring Software. (n.d). Retrieved from <http://webwatchernow.com> ■

### Earn CE Credit

To earn CE credit, complete the exam for this article on page 50 or complete the exam online at [www.acfei.com](http://www.acfei.com) (select "Online CE").

## ABOUT THE AUTHOR

**Louis L. Akin, LPI**, is a licensed professional investigator and member of ACFEI in Austin, Texas, with 23 years experience in crime scene investigation and reconstruction. Akin designed and engineered the *On Scene Blood Spatter Calculator* software that automates recording and calculating blood spatter and authored the pocket manual *Blood Spatter Interpretation at Crime and Accident Scenes: Step by Step Field Guide for Medicolegal Investigators*, which offers a simplified method of manually collecting, recording, and preserving blood spatter data on scene. [www.akininc.com](http://www.akininc.com)





**ATTENTION ACFEI MEMBERS: Journal-Learning CEs are now FREE when taken online. Visit [www.acfei.com](http://www.acfei.com).**

## TO RECEIVE CE CREDIT FOR THIS ARTICLE

In order to receive one CE credit, each participant is required to

1. Read the continuing education article.
2. Complete the exam by circling the chosen answer for each question. Complete the evaluation form.
3. Mail or fax the completed form, along with the \$15 payment for each CE exam taken to:  
ACFEI, 2750 East Sunshine, Springfield, MO 65804. Or Fax to: 417-881-4702. Or go online to [www.acfei.com](http://www.acfei.com) and take the test for FREE.

For each exam passed with a grade of 70% or above, a certificate of completion for 1.0 continuing education credit will be mailed. Please allow at least 2 weeks to receive your certificate. The participants who do not pass the exam are notified and will have a second opportunity to complete the exam. Any questions, grievances or comments can be directed to the CE Department at (800) 592-1399, fax (417) 881-4702, or e-mail: [cedept@acfei.com](mailto:cedept@acfei.com). *Continuing education credits for participation in this activity may not apply toward license renewal in all states. It is the responsibility of each participant to verify the requirements of his/her state licensing board(s). Continuing education activities printed in the journals will not be issued any refund.*

## CE ACCREDITATIONS FOR THIS ARTICLE

This article is approved by the following for continuing education credit:

(ACFEI) The American College of Forensic Examiners International provides this continuing education credit for Diplomates.

## LEARNING OBJECTIVES

After studying this article, participants should be better able to do the following:

1. Understand the various ways that eavesdropping can be accomplished by modern technology.
2. Guard against illegal eavesdropping.

**KEYWORDS:** key loggers, wiretaps, bugs, transmitters, Trojans

**TARGET AUDIENCE:** Security professionals

**PROGRAM LEVEL:** Basic

**DISCLOSURE:** The author has nothing to disclose.

**PREREQUISITES:** None

## ABSTRACT

Thanks to the hefty law enforcement and civilian security budgets that drive the industry, eavesdropping technology has been booming for three decades and invasions of privacy are easier to accomplish today than in any time in history. Cell phones can be turned on remotely to listen to live conversations. Carrier current monitors can be attached to electrical house or office wiring to listen to what is being discussed inside. Keystroke loggers can be attached to or installed in computers to capture every password that is typed and every e-mail that is sent or even read. Small GPS locators can be placed on cars or motorcycles to monitor by remote computer every place the vehicle travels and record the exact address of each stop—and it's all done in real time. It's so easy to do that it's hard to resist doing it, legally or illegally. Who is going to know? This article is for law-abiding people would like to learn some of the technology available and how it is utilized. Just because you're paranoid doesn't mean someone isn't eavesdropping on you.

## POST CE TEST QUESTIONS (Answer the following questions after reading the article)

### 1 Taps are devices that are placed

- a. on telephone lines for purposes of covert eavesdropping.
- b. on computer lines for keystroke capture.
- c. in rooms to capture conversations.

### 2 Bugs are devices placed

- a. on telephone lines for purposes of covert eavesdropping.
- b. on computer lines for keystroke capture.
- c. in rooms to capture conversations.

### 3 Transmitters are easy to hide because of their small size, but

- a. they require entry to the target area to plant.
- b. the distance they can transmit is limited by the small speakers.
- c. they have to be hard-wired to the target area and removed afterwards.

### 4 Eavesdropping devices can be physically installed on cell phones or computers

- a. in a matter of minutes by an intruder.
- b. by sending them to the target via regular mail or UPS.
- c. only if the computer or cell phone is taken in for repair.

### 5 Carrier current devices are

- a. illegal under federal law.
- b. sold as baby monitor systems in electronic sources.
- c. only legally available to law enforcement officers.

### 6 Key loggers give a third party access to

- a. every file and document on a target computer's hard drive.
- b. any stroke of the key which can be replicated on the eavesdropper's computer screen.
- c. what the target says in e-mails, instant messaging, documents, and spread sheets.
- d. all of the above.

## EVALUATION: Circle one (1=Poor 2=Below Average 3=Average 4=Above Average 5=Excellent)

If you require special accommodations to participate in accordance with the Americans with Disabilities Act, please contact the CE Department at (800) 592-1399.

- |  |           |
|--|-----------|
| 1. Information was relevant and applicable.  | 1 2 3 4 5 |
| 2. Learning objective 1 was met.   | 1 2 3 4 5 |
| 3. Learning objective 2 was met.   | 1 2 3 4 5 |
| 4. You were satisfied with the article.  | 1 2 3 4 5 |
| 5. ADA instructions were adequate.   | 1 2 3 4 5 |
| 6. The author's knowledge, expertise, and clarity were appropriate.                | 1 2 3 4 5 |
| 7. Article was fair, balanced, and free of commercial bias.                        | 1 2 3 4 5 |
| 8. The article was appropriate to your education, experience, and licensure level. | 1 2 3 4 5 |
| 9. Instructional materials were useful.  | 1 2 3 4 5 |

## PAYMENT INFORMATION: \$15 per test (FREE ONLINE)

Name: \_\_\_\_\_ State License #: \_\_\_\_\_

Phone Number: \_\_\_\_\_ Member ID #: \_\_\_\_\_

Address: \_\_\_\_\_ City: \_\_\_\_\_

State: \_\_\_\_\_ Zip: \_\_\_\_\_ E-mail: \_\_\_\_\_

Credit Card # \_\_\_\_\_

Circle one:  check enclosed  MasterCard  Visa  American Express

Name on card: \_\_\_\_\_ Exp. Date: \_\_\_\_\_

Signature \_\_\_\_\_ Date \_\_\_\_\_

Statement of completion: I attest to having completed the CE activity. Please send the completed form, along with your payment of \$15 for each test taken. Fax: (417) 881-4702, or mail the forms to ACFEI Continuing Education, 2750 E. Sunshine, Springfield, MO 65804. If you have questions, please call (417) 881-3818 or toll free at (800) 592-1399.