

Activity Monitors aka: Eavesdroppers

By Louis L. Akin, LPI

A lawyer and his client 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 lean forward for a highly confidential tête-à-tête. They are not the only ones interested in their discussion, and, unknown to them, a third party miles away remotely turns on the lawyer's cell phone and records every word of the conversation. When the conversation ends the lawyer turns on his phone, calls his investigator and gets the latest on statements taken from key witnesses. The third party records that conversation too, and while she is at it, downloads all the text messages and e-mails the lawyer has on his cell phone. She also downloads the telephone numbers, dates, exact times, duration of the conversations, and the locations at which the lawyer was at for every call that has been placed or received on his cell phone for the past month. Fantastic? Not at all. 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. Nowadays, 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 doesn't prohibit itⁱ.

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 that had one installed on it (which required a previous burglary to install) 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 incredible small size, but they still require entry into the target area to plantⁱⁱ. San Francisco private investigator, Hal Lipset, waltzed around a cocktail party in the 1960s with a transmitter hidden in an olive in his martiniⁱⁱⁱ. The toothpick was hollowed out for the antennae. Considering that he did it at about the time that color televisions were beginning to appear in homes in America, this was a considerable feat.

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 then transmit them through the air in short bursts that hop about

in a preset pattern amongst multiple frequencies^{iv}. 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, client, sales person, acquaintance, cop in black, 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." When the consumer calls to get the update they get 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 room conversation or autodial 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.

FlexiSpy Products' \$49.95 FlexiSpy Pro^v spyware cell phone tap 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. Now, since most of us wear our cell phones on our belts...

FlexiSpy Products advertises it's product as the "World's Most Powerful Spy Software for mobile phones. FlexiSpy Pro^{vi} is a mobile phone monitoring application that secretly records all activity on a mobile phone that has FlexiSpy Pro installed. Protect your children, catch cheating spouses, the possibilities are endless.^{vii}" The possibilities for abuse are endless, too.

According to the FlexiSpy Products 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."

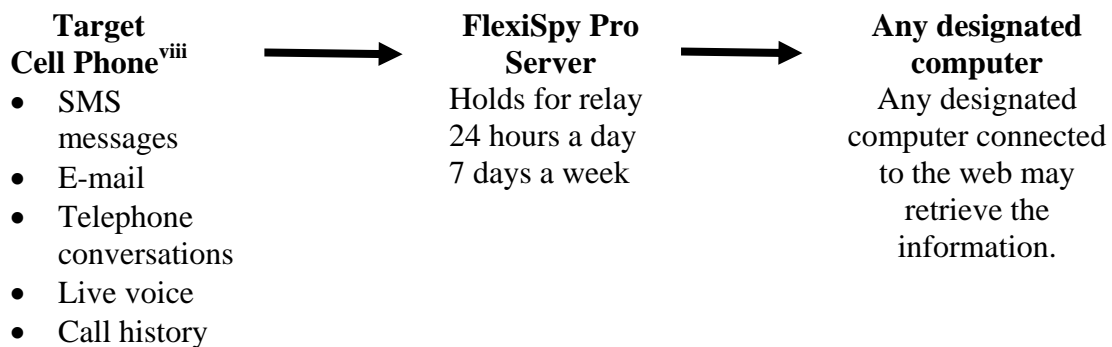
Actually, it's plainly illegal to use the tap on anyone except your minor children. FlexiSpy Products adds the limp caveat

“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 PRO on an unsuspecting neighbor, that's a different story altogether.”

FlexiSpy Products adamantly denies that FlexiSpy Pro tap is a Trojan stating that it has to be consciously installed by a real 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, 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:



F-Secure warns consumers:

“When FlexiSpy Pro 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 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 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 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.^{ix}”

Law enforcement has a more limited but more easily installed cell phone tap. Once they get your cell phone number they go to a website to find who the service

provider is. 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 too 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 cells 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, that is disposables. Disposables are transmitter bugs that can be left somewhere to transmit until their battery runs dry and 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. They 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 plug in intercom systems do the same thing and are used by eavesdroppers for the same purposes. They are also commonly available in electronics stores.^x More sophisticated devices include light switches and wall plugs that really work to turn on the lights or run the vacuum, but 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. It fits in line and looks like part of the cable in the back of the computer. 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 which 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, and 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 pays on line.

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. FlexiSpy Pro 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! ^{xi}”

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

Wireless Connections Even More vulnerable

Wireless computer systems are more vulnerable than the land line or phone lines systems. A wireless computer is essentially a small broadcaster just like a commercial radio tower that broadcasts to car radios, but weaker. The user's computer broadcasts to the receiver which then connects to the internet.

The regular computer key logs will work on a wireless computer, but there is an easier way to capture the user's every key stroke. It's as simple as having another receiver in the area tuned to the same frequency. The broadcast frequency is easy to find with a frequency counter or other devices made for that purpose.

ISIS's Sk-05 Wireless Key Capture surveillance system is designed to offer an eavesdropper a covert means to record keystrokes originating from a computer whose user is under surveillance. The information gathered can include typed documents, passwords, outgoing emails, websites, outgoing internet messaging, etc. The eavesdropper may be sitting in a car outside the building or in the café two floors below.^{xii}

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

Conclusion

Eavesdropping is probably more common today than any time in history. 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 doesn't mean that someone isn't following you." Now we can add: "...listening to every word you say and watching every word you type."

ⁱ Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. § 3789d,

ⁱⁱ Electronic Surveillance Countermeasures, Jarvis International Academy

ⁱⁱⁱ Holt, Patricia The Bug in the Martini Olive, Random House Value Publishing 1993

^{iv} Electronic Surveillance Counter measures, Texas A&M Extension Services,

^v FlexiSpy Products and FlexiSpy Pro are not the real names of the products being discussed.

This author does not intend to advertise the products in any way.

^{vi} FlexiSpy Pro is not the real name of the products being discussed. This author does not intend to advertise the products in any way.

^{vii} WebWatcher Computer Monitoring Software

<http://www.awaresstech.com/employees/index.html?sid=30> ,

^{viii} F-Secure Trojan Information Pages : <http://www.f-secure.com>

^{ix} F-Secure Trojan Information Pages : <http://www.f-secure.com>

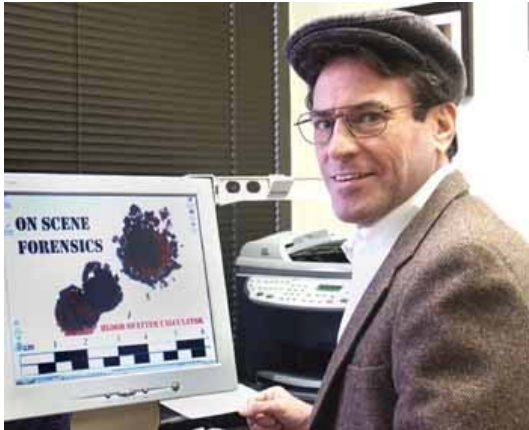
^x Wiretapping and Electronic Surveillance, National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance, GPO 1976 Washington DC

^{xi} WebWatcher Computer Monitoring Software

<http://www.awaresstech.com/employees/index.html?sid=30>

^{xii} ISIS's Sk-05 Wireless Key Capture surveillance system. <http://www.isis.com>

Author's biography



Louis L. Akin is a licensed professional investigator and owner of Akin Investigations in Austin, Texas. Akin was recently awarded the coveted Meritorious Award for Excellence in Investigations by the Texas Association of Licensed Investigators for his work in catching an eavesdropper in the act. As a result of Akin's investigation the wire tapper is currently serving a sentence of five years in prison. Akin attended both the Texas A&M and Jarvis International Academy technical surveillance schools and has been performing electronic sweeps for twenty-five years.