

Who's Afraid of the BBW?
Louis L. Akin, LPI

Who's Afraid of the Big Bad Wolf? Technical Surveillance in the Age of Homeland Security

*"What big ears you have, Grandma," said Little Red Riding Hood.
"All the better to listen to your private conversations with," answered the Big Bad Wolf.
"What big eyes you have," said Little Red Riding Hood.
"All the better to search you with my dear," answered the Big Bad Wolf.
"What a big nose you have, grandma" said Little Red Riding Hood
"All the better to sniff you out, dear," answered the Big Bad Wolf
"What big teeth you have," said Little Red Riding Hood.
"All the better to seize you with," said the Big Bad Wolf.*

*Jakob and Wilhelm Grimm
(Slightly paraphrased by author)*

Terms:

Bug: an electronic device, usually a radio frequency transmitter, wired mike, or carrier current device used to pick up room conversation.

Tap: a device used to listen to and usually to record telephone conversations.

GPS: global positioning system, satellite surveillance to keep track of a person or vehicle, accurate to within 30 inches.

Once upon a pre-silicon time, big ears and eyes were a dead giveaway for a predator who was trying to gain information about his, or her, prey. In Grimm's fairy tale the wolf wearing Grandma's night gown may have been a ridiculous sight, but what else could he, or she, have done in the situation? In those days, Big Bad Wolves (BBW's) and Little Red Riding Hoods (LRRH's) had to rely on guile and the body parts that nature provided them to snare prey. Not so anymore. Silicon has enhanced the weaponry of both sides. Though most of us no longer fear BBW's, some people have an even greater fear of Big Brother (BB) and strain at an interpretation of Jakob and Wilhelm's story as a metaphor of totalitarian security gone awry. This article will survey silicon enhancements of covert surveillance technology—the miniaturization of the wolf's big eyes and ears—and how BB might use them.

Jarvis International Academy, run by Ray Jarvis, a retired CIA agent, is a highly respected training school for technical surveillance and surveillance countermeasures. The Academy offers 2-week basic and advanced countermeasures (TSCM) courses to law enforcement and non-law enforcement personnel. For law enforcement agents they offer several additional courses on topics such as: How to bypass burglar alarm systems to gain covert entry; How to pick locks; How to tap telephone lines; How to install mikes and transmitters in household electrical wiring systems; How to pick sound out of the air and transmit it to a listening post; and how to implement covert video surveillance. The wiretaps may be placed on telephones inside the house, or office, or half mile away at the junction box, in fact, anywhere between the target and the telephone central station. Listening posts may be located anywhere from a quarter mile to four miles or more away. In fact, they can be infinite miles away, as far as satellites can beam them.

Since the 70's and 80's, schools like Jarvis, the Texas A&M Engineering Extension Center TSCM school (not presently active), and other schools across the country began

graduating hundreds of law enforcement electronics surveillance and counter surveillance agents each year and they trained as many civilian agents, mostly former law enforcement, for the security departments of major American Corporations. Some Las Vegas casinos even sent their security personnel to learn the technology of bugging and debugging. The majority of the graduates of the schools, then and now, consist of active law enforcement agents from state, county, and municipal departments. The feds have their own academy called FLETC or Federal Law Enforcement Training Center, in Glynco, GA (don't look for it on a map), where federal state, county, and municipal law enforcement agents can attend classes. They provide training for non-law enforcement corporate security personnel too:

“The FLETC was created to train federal law enforcement officers. . . Private sector students can be admitted if the admission criteria is (sic) satisfied and a Partner Agency sponsors the student.”

There have been rumors that some agents of these schools, having been trained to disable burglar alarms, pick locks, and surreptitiously enter homes and businesses in the still of night to install listening and watching devices in every room and on every telephone and computer, have learned that important intelligence could be gathered with surveillance technology without a warrant. Even if the information couldn't be used in court when it was obtained without a valid search warrant, it was still usable information that could lead to arrests and probably could be chalked up to “an anonymous informant who has provided reliable information in the past”

Today, law enforcement has the technology to listen and watch the private conversations and actions of anyone they choose. Field Effect Transmitters (FET) not much larger than the top part of this exclamation point ! that use wire the thickness of fine human hair can be sewn into curtains, carpets, or clothes, even painted onto walls or other surfaces. Wireless RF transmitters can be inserted in the head rests of cars or office chairs. They can be disguised as wall sockets, light switches, calculators, garage door openers, radar detectors, pagers, cell phones, picture frames, pens, and artificial plants, even hidden in credit cards according to one source. Video cameras can be hidden in shirt or coat buttons, neckties, reading glasses, and Phillips head screwsⁱⁱ. Styrofoam cups from coffee machines have been used as transmitters (water is a great conductor of sound). The devices can transmit video and audio to a nearby receiver that can record it digitally or relay it for miles to be recorded elsewhere.

Tracking transmitters that use cell phones and GPS satellites can track a car or person anywhere in the world recording his whereabouts and giving his position on the earth within less than a meter—30 inches. The person's cell phone doesn't even have to be on. Many GPS tracking transmitters work the same way and just as accurately. Thermal imaging, electret, shotgun, and parabolic mikes and laser beams are used in bugging, and the variety of ways to tap telephones is too long to list in this article. Key logging software or hardware will record every key stroke made on a computer, capture every password used, record every web site visited, and send copies of every document typed,

or e-mail sent and the full text of instant messaging to a surveillance agent's computer miles away.

The information used to snare prey doesn't have to come from live technical interceptions. Some of it is stored in records that can be inspected once someone comes under suspicion. Take, for instance, cell phone records.

Cell phone antennas are set up on a Doppler style system along highways and main roads. By using cell phone records the police can retrace a person's route and determine to the hundredth of a second where the person was, what direction he, or she, was traveling, the street they were on, even how fast they were driving. In an emergency, such as a terrorist attack or mutinous walkout of the legislature, the police can access a person's present movements to track them. The old trick of calling a third party's cell and having them call another person for a conference call was never a trick that worked, because every cell phone that comes into the conversation is recorded by the cell company. The records even show who called who (or at least whose phone called whose) where each caller was, and, again to the hundredth of a second, how long they talked. If they were both driving around at the time, the records will show where each of them drove.

In the meantime, the less sophisticated but highly effective and reliable technology of the 80's and 90's have proliferated into a glut of eavesdropping devices available to the general public and used more than one would think by law enforcement. The advantage of low cost over-the-counter gadgets is that most of it doesn't have serial numbers, and so many are sold that they are impossible to trace. For instance common baby monitors can be converted into carrier current devices that use the existing 120 volt wiring in a house or office much like a telegraph line was used to send messages, but now the messages contain live audio, even whispered words, instead of Morse code. Carrier current transmitters can be hidden in light switches, electric sockets, lamps, computers, or any appliance that plugs into a wall socket and the appliance will work just like it always has.

The profusion of available bugging and tapping devices resulted in an explosion of electronic eavesdropping in the 80's and 90's that quickly mutated into audio-video eavesdropping in the late 90's and continues today in more and more sophisticated ways. Movies like Francis Ford Coppola's *The Conversation* with Gene Hackman showed the leading edge in bugging technology of the 1970's much of which is still in use today such as electret, spike, and parabolic mikes, concealable transmitters. The movie ended, appropriately, with the appearance of something new and undetectable at the time, which could have been a frequency hopper or burst transmitter, or a transmitter that operated on a frequency higher or lower than the countermeasure equipment of that day could reach. (Frequency hoppers change frequencies as they transmit information and burst transmitters store information to send it out in short bursts.)

Just as bugging and tapping devices have proliferated and changed since Coppola's classic movie, so has the equipment used to perform electronic surveillance counter measures, colloquially "debugging sweeps." To the chagrin of some amateur "debuggers" who attempt to perform countermeasure sweeps without having first obtained the

necessary training, much of the new equipment is poorly designed and some of it intentionally poorly designed and sold by companies who understandably don't want their own bugs and taps found.

Lawyers, investigators, and their clients should be cautious of amateur "debuggers." The amateur debugger may announce with authority that a room is or isn't bugged when in fact they don't know if it is or not, because their equipment can't tell them whether they are detecting an RF transmitter, wireless video signal, the local cab company dispatcher, or picking up a local Oldies but Goodies radio station.

The countermeasures business is much more expensive to undertake than bugging. For \$200 worth of equipment a eavesdropper can tap all the telephones in an office or home and bug all the main rooms with carrier current devices and drop bugs, and have enough left for a cheeseburger and fries. The minimum outlay for high quality countermeasures equipment begins in the thousands. The higher level of interception with which a person is threatened, the more expensive is the equipment needed to detect the bugs and taps.

Countermeasures experts generally agree that there are four levels of surreptitious interception operationsⁱⁱⁱ. The most sophisticated, level four, includes the uses of lasers, FET mikes, micro miniature video cameras, and transmitters that operate in the high gigahertz (2.4+) frequency range. The equipment is costly and is mostly confined to the federal government, the larger law enforcement agencies, and the security departments of large corporations who can afford it. Level two and three operations are performed by local police agencies and private investigators and are the most active levels. Level one is what husbands, wives, parents, and people with camcorders and micro cassette tape recorders do.

The explosion in bugging has come at levels two and three, with the most volume at level three. Private investigators in the 70's and 80's speculated that the public and private subcultures of surveillance agents would not last, because lawyers would sue them into extinction. That hasn't happened. Either lawyers don't bother to have their own or their client's offices, homes, and cars swept, or they are hiring the guys with the \$89 "bug detectors" who are missing the bugs and taps and don't know it.

The question has become, Who's afraid of BB, and does a citizen need to construct a soundproof brick fortress to have privacy? The answer is that interception proof fortresses are expensive and usually don't work. So, if you're going to have a conversation that you really want to keep confidential, have it in person, outside your office building, preferably at a busy place where you do not usually go for lunch or coffee or drinks, speak in code in low tones, and don't use the same place twice. Or have your office swept regularly by someone who knows how to do it right. The minimum equipment that the debugger will need includes an RF detector with a range of 1MHz to 2.5 GHz or higher, a frequency counter with the same range, an audio analog receiver that can scan the same range of frequencies, a device that will demodulate intelligence being transmitted by carrier current devices, equipment to check the telephone lines for

taps, and software to sweep the computers for key loggers. By the way, don't contact that person from the place you want swept.

ⁱ www.FLETC.gov

ⁱⁱ Supercircuits Catalog #51 2004

ⁱⁱⁱ Swift, Ted, former DEA, Texas A & M University Extension Center, Electronic Surveillance

Sidebar 1

The history of technical surveillance is a relatively short one. While surveillance agents had long been able to tap into a telephone line to listen to the conversation in a home or office, they were limited to a direct connection to the line being used. In 1950, a private investigator by the name of Manny Middleman invented a telephone wiretap that could be activated by a tone sent from another telephone anywhere coast to coast. It was the first *infinity* transmitter, aka, the harmonica tap, because Middleman used a harmonica to make the tone that activated the tap.

In the 1960's a San Francisco private investigator named Hal Lipset invented the "olive in the martini" RF transmitter bug using a hollowed toothpick as an antenna. Spike mikes, parabolic mikes, drop bugs, and hook switch bypasses (altering a telephone in an office so that it becomes a live microphone even when on the hook) were on the scene and eavesdropping devices began to multiply as government agents and private investigators vied for new devices as fast as they appeared on the market, or invented their own.

It was a highly secretive market and an expensive one. It remained so until the early seventies when eavesdropping devices found their way from the hands of CIA agents and private investigators into the desk drawers and jacket pockets of every law enforcement agency in the country. The demand by law enforcement for taps and bugs has created a billion dollar industry that produces a plethora of taps, bugs, and video cameras, mostly remote controlled, and all micro-miniature, thanks to silicon enhancements.

Sidebar 2

While writing this article, the author received this email. Private investigators and others receive these kinds of advertisements regularly, by mail and by electronic mail.

March 6, 2007

To: **Akin Investigations**

From: **Marco Lomeli**

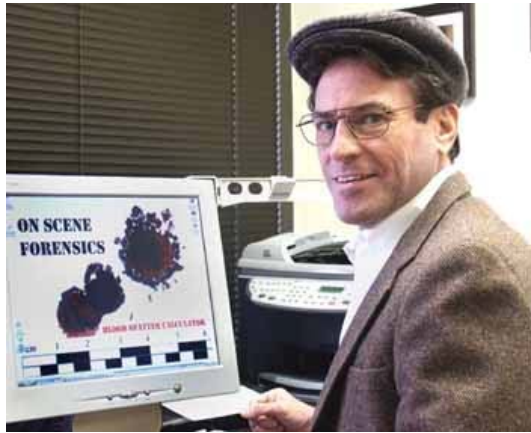
Company: **PCPandora**

Subject: **monitoring tool**

Hello, I just became aware of your private investigation services, and I was curious to know if your clients would be interested in using our Internet monitoring tool called PCPandora.com I would also like to give you a free copy so you can test it out right away. PC Pandora is a great tool that spouses can use to see if their husband/wife is

cheating on them. PC Pandora secretly records all of the following: * Every website visited * All EMAILS sent and received * All INSTANT MESSAGES sent and received * All CHAT ROOM conversation * Every PROGRAM that is run * Every KEYSTROKE typed will be recorded The best feature of the software is that you can set up the program to send you reports every 20 or 30 minutes directly to your email. These reports contain everything that has been done on the computer that you're monitoring; you will be able to read the emails and IMs that were sent/received and everything else. It's a great product, and a perfect fit for your services. Please let me know if you would be interested in testing out a free copy. Thank you! Marco Lomeli Mlomeli@PCpandora.com

Biography



Louis L. Akin is a licensed professional investigator and owner of Akin Investigations in Austin, Texas. Akin is a Certified Criminal Defense Investigator by the Texas Criminal Defense Investigator's Association and was recently awarded the 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 eavesdropper received 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.