

## Brief Bio:

TSCM technician and Private Investigator Louis L. Akin's first involvement with countermeasures sweeps was when a woman came to his office complaining that she was convinced that something bad had happened where she worked and that her employer was eavesdropping on her. She worked at 3-Mile Island and turned out to be right on both accounts. Akin began his formal technical countermeasures training at Texas A&M School of Engineering Extension Center in 1987. He continued training at the Jarvis International Intelligence Academy, Tulsa in 1988 and REI International and has continually updated his training. He first testified as an expert on technical surveillance countermeasures in a case filed in the 348th District Court in Tarrant County, Texas in January 1991. Akin has accumulated twenty-two years of experience performing sweeps at levels 3 and 4. In March 2007 Akin, was awarded the Meritorious Service Award for Investigative Excellence by the Texas Association of Licensed Investigators for discovering a wiretap installed on the telephone line of an Austin woman. The discovery led to the arrest and conviction of a 55-year old Austin contractor who had stalked, harassed, and psychologically tortured ex-girlfriends over the past 20-years. Based on evidence that Akin developed, the contractor was convicted of wiretapping and burglary and sentenced to five years in prison. Akin has written articles on TSCM for the American College of Forensic Examiners, the National Association of Criminal Defense Investigators, The Texas Association of Criminal Defense Lawyers, and other magazines including the Texas Investigator.

DPL: How many ways can an eavesdropper bug you?

LA: The ways are nearly endless and widely varied, from light switches or lamps that transmit audio, to cameras that see through pinholes, to hook switch bypasses that remotely turn on your telephone or spyware that remotely turns on your cell phone, to key loggers that allow someone miles away to watch everything you do on your computer screen, to drop bugs that transmit voice or recorders that record only when you speak. And then there's the sophisticated stuff like Styrofoam cups in coffee machines that transmit voice or FET mikes (field effect transmitters) that can be sewn into clothes or painted on walls. And then there is GPS tracking that is becoming too popular for a nation that values privacy. The proliferation of bugging equipment over the last thirty years is a direct result of the huge budgets that law enforcement agencies have been granted to spend on toys. The cops used to have to hire private investigators to plant taps and bugs. Now every police department in any mid to large sized city has officers trained to plant bugs and taps and many of those plants are legally installed, or at least they were before the Patriot Act removed accountability. The 1970's movie "The Conversation" by Francis Ford Copula with Gene Hackman and Harrison Ford is the best film ever done on the world of eavesdroppers and many techniques used in that movie are still employed.

DPL: What's the difference between a tap and a bug?

LA: A tap is placed on a land line telephone, that is, the kind that have a wire running to a telephone pole. A bug is a transmitter that is hidden on a premises or person or vehicle to pickup audio. The software put on cell phones is considered spyware by most. Cameras and videos are a big part of eavesdropping surveillance and are more widely used than straight audio in government applications. One of the coolest video setups I ever saw was literally a pin spec in the middle of a mirror over a dresser in a hotel room. You could look in the mirror all day without seeing it until we detected it with equipment.

DPL: What are the most common methods employed by police and PIs? Which are used by stalkers and other criminals?

LA: PI's and police install lots of different devices including wall switches, clocks, books, lamps, vases and such. They can also install devices that are camouflaged as an ordinary screw or button, a picture frame, etc. Devices are hidden in small hand held calculators, writing pens, flower pots, furniture, and computers, stereos or speakers, in walls, heater vents. Most people have given up on the cameras in baseball caps since agents were bringing back too much video of ceilings, but every other item of clothing is used including neckties and bras. One device is planted in office chairs and is activated when someone sits down. Others turn on when the light switch is thrown on, or voice is heard, or movement is detected. Stalkers and illegal eavesdroppers go more for devices that can be left behind like tiny transmitters that can be stuck above a ceiling tile, or in a wall, or in furniture. Recorders are always a big threat at the amateur level.

DPL: What exactly is phone tapping and how is it done? Does the tapper need physical access to the victim's phone or can it be done wirelessly?

LA: A tap is a device that allows an eavesdropper to listen to and record conversations that are held on a telephone, wireless phones included. Telephone taps can be installed on telephone lines anywhere between a house or office and the relay station. The cops install their legal taps right at the telephone company. The illegal ones can go on telephone poles, on outside wiring, in telephone rooms, in key boxes, or in the actual telephone instruments. PI's can install legal devices in the latter fashion. Some install illegal ones in the same way. Let me throw in that if you have an illegal tap on your telephone line and call the telephone company and they find it, they will remove it but they won't admit they found one. The problem is that the eavesdropper can come back and replace it. Telephone taps are available at any Radio Shack store<sup>1</sup>.

DPL: What about these cell phone tapping companies that advertise on the internet? Are they reliable? Do their systems work? Can someone use them anonymously?

LA: If you mean companies like Flexispy and others I've written about they are software programs that can be installed on cell phones. Yes they work, but while the sellers

---

<sup>1</sup> The consensus is that Radio Shack is the biggest supplier of devices used by law enforcement and PIs for eavesdropping. They are non-traceable. You just have to know how to employ them.

advertise them for legal purposes half the uses they list are illegal in most circumstances.

DPL: How would law enforcement or a PI track down the cell phone tapper?

LA: The hard part is finding the tap either by resistance on the phone line or a drop in voltage, or other symptoms. Once you find the tap, the victim usually has a good lead on who the tapper is and most of the time it's a matter of setting him or her up. In one case I found a tap on a telephone that the cops had been called to find five times before. It took me an hour. The tap with a recorder attached to it (both from Radio Shack) was beneath the crawl space of the house. I set the guy up, told the cops when he would return to get the recorder and when he crawled out from under the house with the tape in his hand three flashlights shined in his face. He had stalked other women and wound up getting five years in prison.

DPL: What is a keystroke logger and how does it work? Does the bad guy need physical access to the victim's computer or can this be set up via E mails, etc.?

LA: Answer to first question: A keystroke logger is a software program that goes in a computer and hides itself from the computer. Then it transmits every touch of the keyboard to someone else who can sit and watch every word, including passwords and account numbers on their screen. Every key you touch on your keyboard that creates a reaction from your computer causes the same reaction to show on their monitor. If you type Password 123, That will show on their monitor. If you visit a website, that website will show on their screen. If you look at your bank or credit card account, so will the eavesdropper. Answer to second question: The keystroke logger has to be installed on the computer either on purpose by the eavesdropper having access to the computer or inadvertently by the computer owner. I caught a guy living two states away installing a key logger on a woman's computer by sending it in an email. He had to get her to open the email so it would install. We caught him hands down, a federal offense.

DPL: Who is likely to eavesdrop on someone?

LA: In the domestic realm, leaving out what the KGB and CIA are doing, spouses eavesdrop on spouses during marriage and during divorces or separations and immediately after divorces. Same applies to significant others. In some cases, those kinds of eavesdroppers can be physically dangerous. Families spy on members who are about to inherit or who have inherited large sums of money. Business partners spy on each other. Businesses spy on other businesses. Police and prosecutors spy on defense lawyers. I've known of cases of that happening. It isn't uncommon. Corporations spy on each other all the time. Employers spy on employees. I've caught them doing that. Occasionally landlords spy on tenants. Stalkers usually fall in the dating or marriage categories but can be strangers and can be dangerous. Anytime someone is willing to plant bugs or taps in your home or office or car they have to be regarded with caution to say the least. They mean you no good in most instances. Men

are more likely to install devices; women are more likely to ask someone to do it for them.

DPL: Who is likely to be eavesdropped on?

LA: Spouses, girl or boyfriends, employees, partners, people in competition with other people, PIs, people in business, people involved with law suits or lawyers, celebrities, people involved in criminal activity. There is usually a rational reason and it usually isn't the CIA. I reject the CIA victims outright.

DPL: How do technicians categorize eavesdroppers as to their level of sophistication?

LA: There isn't really an industry standard that I am aware of, but a lot of technicians break it down into four levels:

1. National security, military, etc.
2. Corporate security, federal law enforcement
3. Small business, law firms, ordinary people getting married or divorced, people using drugs, PIs, local law enforcement.
4. Idiots with tape recorders.

DPL: What about IR and laser bugs? How do they work and what can they do and not do? How would someone know these techniques were being employed against them?

LA: Infrared and laser technology is used in bugging. They are beams of light. A lot of times they are used to activate devices or turn them on or off. The laser bug against the window of a high rise building is actually very limited. It's supposed to pick up the vibrations of the people talking inside, but if you add in the vibrations on the window caused by buses and trucks passing, cars honking, airplanes flying over, and people talking outside you can see the problems. Detecting them can only be accomplished with equipment designed specifically to pick up their frequencies of light.

DPL: Your office is in Austin, Texas, How many private investigators in Texas actually use these tools and/or help someone discover if they have been bugged or tapped?

LA: In Texas, there are only about a half dozen private investigators who are qualified to do technical surveillance countermeasures sweeps which is the industry terminology for debugging. By qualified, I mean that we have had formal training in bugs and taps and debugging, that we use equipment that can actually detect eavesdropping devices, and that we have at least three years of experience in performing sweeps. Most PIs can't pass the first to qualifications. They have no training and no idea what kinds of taps and bugs are out there. Second, they don't have the expensive high quality equipment necessary for finding eavesdropping devices. They'll buy an \$89 "bug detector" or "tap detector" at a spy trinket store and start selling their services to the public. Another type of investigator advertises that he or she can do sweeps and then hires one of us to do the sweep. In that case, the PI is just inserting himself as a middleman and taking a cut

which has to be added to the cost of the sweep. It's cheaper and more reliable to go straight to a TSCM technician. There is a non-profit technician referral service at [www.tscmtech.net/](http://www.tscmtech.net/) Any PI who satisfies those criteria can get listed on it. We refuse to list any who don't. So far, there are only a half dozen.

The site was created to protect the public from false, misleading, and deceptive advertisements by PIs who wouldn't know a tap from a knock. There are legitimate TSCM experts in El Paso, Dallas, Austin, and Houston areas. Most of the technicians will work anywhere in the state and some in other states as well.

*DPL: Any interesting stories?*

*LLA: Unfortunately, this kind of work attracts a lot of paranoid schizophrenics. I try to get them to seek help, but I don't think I've ever been successful at it. A humorous story was when a huge burly guy in bib overalls came into my office saying he was being followed by helicopters. He had been arrested for getting out of his car in a street and challenging a pilot to land one and fight him like a man. I turned him away and as he was going down the elevator leaving my office my wife called to inform me that someone had reported a sniper on the building across the street from mine. She said the police and television helicopters were flying all around my building. It turned out to be a false alarm, but at the time I wondered how the guy I turned away would react when he came out of the building and saw them. It crossed my mind that he might come back up the elevator looking for me as a co-conspirator.*

*Most stories of schizophrenic people are tragic though, because, to them, the whole thing is real. They really are being followed and watched. To them it's as real as rain. Some lay awake at night. One terrible case involved a brilliant young engineer who came to me and offered to pay \$5000 up front for a sweep. I refused his case, but tried to help him by encouraging to get back on his meds each time he would come to visit me. He started back on them, he told me, but was under medicating because he didn't like the side effects. About six months later he killed himself and his wife and left three beautiful young daughters behind. I've never forgotten that guy.*