

Lee A. Denney

Private Investigator

(919)847-3344

184 Wind Chime Ct.

Raleigh, NC 27615

Fax: (919)847-3342

www.ncPrivateEye.com

CELL PHONE BUGGING

Not long ago, I was asked by a well-known Criminal Defense Attorney if a cell phone could be turned into a “Bug”. In this particular instance the attorney had a client who had been picked up by a Federal Agency and was subsequently charged. Shortly after the client was released, the Feds returned his cell phone to him.

The concern the client and the attorney now had was this: why had the Feds waited some period of time before giving his cell phone back and was it now a bug? Initially the attorney could not get up with me so he called another PI and asked him if the Feds could have put a bug into the cell phone. This PI said he could take the phone apart and check for bugs, however he would have to take the phone away from the attorney’s office. Thankfully the attorney did not do this and was able to contact me.

A little common sense mixed with having taken cell phones apart in the past told me if the phone had been turned into a bug, it was not done by putting something into it. There is no room in a cell phone for anything other than the guts of the phone, the battery and sometimes a larger memory chip. To put a microphone into a cell phone and have it powered would take a magician. In addition, a cell phone is already a microphone and transmitter. All portable telephones, cell or otherwise are transmitters.

When I get called to check someone’s home for hidden transmitters and bugged telephones, the first thing I find are wireless handsets. These wireless handsets are transmitters and are transmitting over airwaves. Anyone with the proper receiver and is within range can listen in on the conversation. No extra “bugging” has to be done. When I tell clients this they are shocked and amazed. I use the stories of people with baby monitors in their house and the neighbor next door being able hear their baby monitor from within their own residence either on their own baby monitor, telephone or another type of receiver.

I have also had the opportunity to watch what technicians do with malfunctioning cell phones at their shops. I knew they had the ability to update the telephone’s software by essentially plugging it into a computer. They can re-program cell phones in this same manner.

In doing research concerning this subject I found information that backed up what I thought. A cell phone is a miniature computer. Instead of “Software” it is run by what is called “Firmware”

(a program that is embedded in a device). This Firmware can be formatted or reprogrammed making the cell phone a “Bug” without having to put anything in the body of the cell phone.

How is this done? There are two ways to accomplish turning your cell phone into a bug. One method is done by the Feds themselves, using the same computer programming equipment that the cell phone companies use. The other approach is when the cell phone companies do it at the request or subpoena of the Federal Agency. This then allows them to turn the “bugging feature” now in your Firmware on and off when they choose. To further complicate matters, some of the newer phones can have their Firmware remotely changed, which means it can be done while it is in your possession.

How do you deal with this possibility? The only way to make the cell phone unable to transmit or work as a bug is to take the battery out of the phone. Merely turning the phone off still leaves power in the phone, making it possible to turn the phone on without your knowledge.

How do you find out if your cell phone has been turned into a bug? There is no single way other than to have a “countermeasure sweeper” with you 24/7. A combination of things will help determine if your phone is bugged. No, I am not going to tell you how you can do these things. Instead, you need to hire me.

One more thing, GM’s OnStar works as a cell phone. It can also be modified to work as a bug.