HOW CELL PHONE DETECTION SYSTEMS WORK

By Robert Burchett; Certified Communications Engineer
Enterprise Electronics www.CellBusted.com
22826 Mariposa Ave. Torrance CA 90502 310.534.4456

Most everyone knows how a metal detector works by now; in simple terms, you walk between the bars, the magnetometers **SEND** some magnetic energy to objects on your person, the item disrupts the magnetic field, the detector senses this and alerts. This is the same for detectors from $100 to $10,000

Cell Phone Detectors work exactly the opposite; they **LISTEN** for the radio signals that come out of the phones. This is completely different and so it is helpful to explain how to deploy them and how they can be a major part of your security procedures to do the best possible job. When in doubt CALL first!

What they WILL detect upon:

- Hearing a phone sending a text
- Hearing a phone receiving a text (they respond back to the sender)
- Making a call
- Receiving a call
- Registering on the cellular network (more about this later)

What they WON'T detect upon:

- **Power OFF:** Phone is OFF (the transmitter sends nothing, so no cell phone detector can hear it)
- **Passing by:** The phone is ON and the wearer simply walks past the detector (but the phone sends nothing at that instant in time since you aren't texting or talking) and that random registration burst probably won't happen exactly at that moment either…these are not "metal detectors" so they can't detect a phone not sending anything nearby. Nothing sent; nothing detected.
- **Bluetooth:** The detectors also won't hear Bluetooth; that is a "paired" communications where the device only transmits the Bluetooth energy under controlled circumstances. So if the phone is ON and their Bluetooth earpiece is paired with it and the phone doesn't ring and you do not make a call then the Bluetooth unit won't transmit; this is done to save that tiny battery inside of the earpiece.
- **WiFi:** The detectors don't hear WiFi for essentially the same reason as Bluetooth; if your facility allows you access to WiFi access points and your phone is turned ON and it is permitted to connect to the WiFi then, and only then, will your WiFi transmitter be permitted to be ON. Of course this detector will also detect the Registration burst since that phone is turned ON and we will catch it to be sure; but NOT because of the WiFi. That isn't ON until you connect to the WiFi access point…which probably won't ever happen inside of a secure facility. Note that if you decide to use your phone to provide a portable "hot spot" to other phones in the area since you aren't permitted WiFi then the detector does pick up the cell phone signal easily.

How phones register on the network and how we use this fact to catch them.

Phones RANDOMLY send 'pings' of short information bursts to the cell network to let it know where they are, request if there are voicemail messages in queue, texts waiting for them, etc. Many of the detectors on the market will not detect these VERY short bursts (about 1/10 of a second) but we do. This is good and bad…here is why:

If you walk past the detector with your phone ON (as previously described) and the phone isn't talking, texting or registering then the detector won't hear it…this is because the phone has a very small battery and regardless of the fact that it is a cell phone, it won't send radio signals until it needs to; if it did then the battery would go dead in an hour and that would not be useful to any of us.

So: when you place the detector *inside* of a secure area AND then when a concealed phone registers on the network we will let you know that it happened. That is a good thing; no metal detector can do this.

These bursts are not at any specific time; we see them from 2 to 5 times per hour; but no one really knows for sure…we just lie in wait for them to ping and then alert you accordingly which a metal detector cannot do as you have to be exactly between the bars in order to have them work…we must use each machine the correct way to get it to perform the job it was designed to do.

When is registration a blessing and a curse at the same time?

Cell phone text & voice calls transmitted signals are a "managed" signal for the most part; this means while you are moving toward a tower the system tells your phone to turn the power down. If you are moving away from it they say turn your power up. This makes your tiny battery last longer and we are all happier for it…but then comes the "curse" part. When a phone "loses sight" of the cell phone network then it is no longer a 'managed' signal and that can be 'induced' by storage in a locker or below ground.

This means that WHEN it does transmit the registration burst (and this can be quite often) the power output will be at MAXIMUM the phone has capability of. Blessing? Sure; that means we can catch them easily. Curse? Yes; that too; since cell phone signals transmit through walls…and everyone knows that.

When can an unmanged phone signal be a problem? Many facilities require that you put your phone in a locker at the front of the building and then the phone usually loses contact with the network. Should the phone be turned ON when in that locker some of them will begin a series of 'cries for help' or constant 'registration' bursting to try and acquire connectivity. This is an unmanaged call and at *full power* which can travel several floors or through many walls as it tries to connect; and a detector placed near it will alert on this signal constantly…this is NOT a "false" alert, the detector is simply doing its job and informing you of the event. Be aware & use it to your advantage; not as a problem or issue to be avoided.

Where else will this phenomenon occur?

Suppose a phone is taken below ground level or inside of any "shielded" environment where it is on the person, powered up and on "standby" but can't connect with the network. This phone can constantly attempt to ping the network with repetitive registration bursts over and over trying to contact the system to no avail. Properly placed and monitored detectors will alert on this and inform you immediately despite the fact that no OUTSIDE signal can get in…and that means the detector is doing a great job of alerting you to the event. Some facility managers ask why the detector alerts in "radio dark" areas and this is why.

Consider that our very expensive ($5000+) metal detectors can't do this at all no matter the threat level unless you specifically walk between the bars, the fact that our highly engineered cell phone detectors WILL alert you to phones in unauthorized areas can be a major component to your security policy…if properly deployed.

Where to properly place the detectors for maximum effect is very important; pay close attention here to get the most out of your security detection system with the maximum policy enforcement:
You *can* install them at the door, in front of the entrance to the secure area BUT be aware that nearby (lobby, street, etc.) phones **are** permitted to be used and these radio signals pass through walls…we expect and demand that they do…so this is no surprise. We just need to take it into account.

If you want the HIGH DETERRENT factor that our detectors are well known for then by all means place one AT the entrance but be sure to turn it down LOW on sensitivity so it doesn't just alert all day long…after a while the personnel will become quite annoyed with it and either unplug it or simply ignore it completely…even if it is telling you exactly what you wanted to know. This is the correct way to implement an effective security policy. Get every bit of the deterrent factor you can and then catch the ones that were missed by placing detectors INSIDE of the secure area. This will maximize the investment.

Suppose you have a secure area/ part of a building/ room/ floor where phones are NOT allowed and it is below, above or adjacent to a NON-secure area where phones ARE permitted to be used (cafeteria, smoke area, restroom, hall, etc.). This creates manageable issues and must be taken into account.

The way to deal with this is to put the detector as FAR away from the non-secure area (don't forget the floor above and below too!) and adjust the detector low enough to try and not hear outside of the protected area while hearing the inside…this is a little difficult and here is why:

How far away will they detect phones? There is no 'finite and specific' distance that phones will be detected. This is due to the variable power output discussed previously. There are 9 steps of power up/ down that a phone will send out when under control of the network so no one knows what power setting the phones are allowed to send at PLUS:

There are several FORMATS of cell phone signals and in order of the most-to-least power being transmitted they are as follows:

1. IDEN (aka: Nextel) has the most power of any digital phone signal (only until next year)
2. GSM (AT&T, T-Mobile, etc.) has the next highest power-per-bit quantity
3. CDMA (Sprint, Verizon, etc.) also known as "spread spectrum" has a lower power per bit
4. LTE/ HSPA and other 4th generation (4-G) types of ultra-wide-bandwidth transmissions

This means that the detectors will alert on a GSM phone when it is farther away than for example a CDMA phone if both are "unmanaged" (at maximum power) or "managed" (variable power but probably lower than full) at the moment of transmission. That makes it difficult to measure exactly where the pickup zones are, how far away we can 'hear' it and alert the incident to you.

Handheld detectors; what they do and don't do:

Handheld detectors are great for certain specific applications; and, like everything, they have capabilities we employ but need to understand them to get the most from their ability. (We don't call it "limitations").

The good parts:

- Portable, easily carried from one area to another, no requirement to be 'fixed'
- Bring the detector to the area of perceived problem immediately
- Lower cost of ownership (they cost a lot less than fixed detectors)
- Hunt down a 'bug' or surveillance device (camera, wireless mike, GPS tracker, etc.)
- Expect a handheld detector to pick these types up; they work and work well BUT:

The bad parts:

- Remember that discussion on the 5 ways phones are detected? Well unless one of these is happening at the EXACT instant you walk by with your handheld detector it won't hear a phone

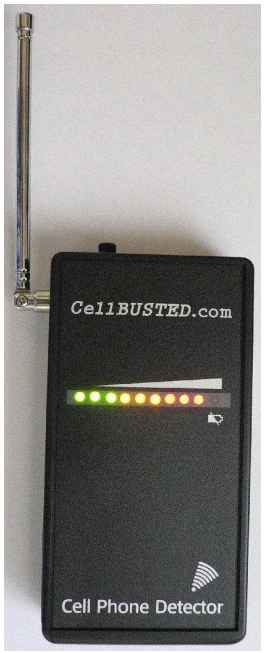
- Sometimes people order the handheld detectors to go and search for people carrying phones against the policy; but are unhappy when they don't detect phones. People see you coming with your detector in-hand and don't send texts or talk on their phone AND if the phone isn't registering then the detector won't find them.
- Don't expect a handheld detector to just find phones in people's pockets for the above stated reasons; use them to find bugs, cameras & trackers that transmit at regular, scheduled intervals.
- Handhelds cost less because they DO less; (you get what you pay for)
- Less filtering inside to screen out 2-way radio signals (usually 'permitted' inside)
- Smaller antenna and only 1 vs. some with multiple antennas = shorter pickup range
- Fewer controls to 'manage' or fine-tune the unit to accommodate environment changes

Get the most out of your security system:

- If you have lockers; put them under control of the guards and make sure phones are OFF
- Put a HIGH DETERRENT kit at the door and turn the sensitivity & volume down lower
- Put detectors INSIDE of the secure area(s) and post the warning signs for maximum effect
- Walk-test the facility inside and out of the secured areas once the detectors are placed
- Keep sensitivity high enough to alert but low enough to NOT detect phones outside
- Want to have the responders notified silently? Order the Silent Remote Option Kits

EXAMPLES OF DIFFERENT TYPES OF CELL PHONE/ RF DETECTORS

Handheld detectors come in different form-factors and pickup/ alert methods. Remember their capabilities and see the differences in the units shown below:

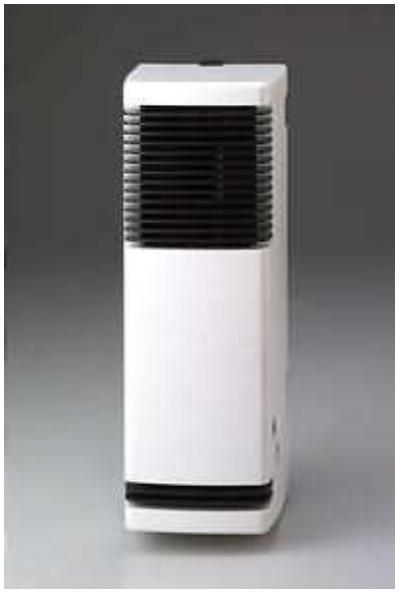


Wideband Unit

Class-Act Classroom Pocket Version

Wideband Unit: One type of ULTRA-WIDE-BAND RF DETECTOR that is quite popular is the Wideband Detector shown. This unit picks up cameras, bugs, surveillance mikes, GPS trackers etc. that use CELLULAR to transmit out

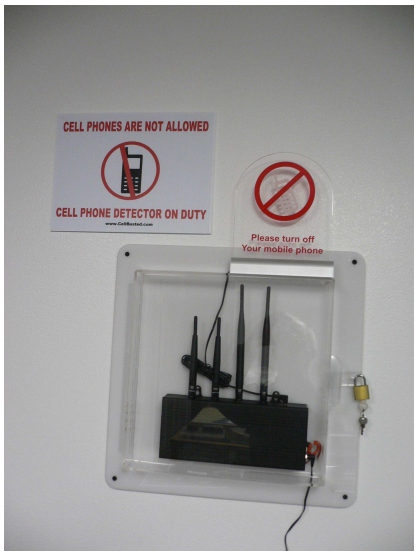
The Class Act (www.Class-Act.net) pocket detector is designed for covert use like in the classroom where instructors want to be alerted to student's improper use of phones. This unit is very small and alerts the wearer to the detection event by silently vibrating.



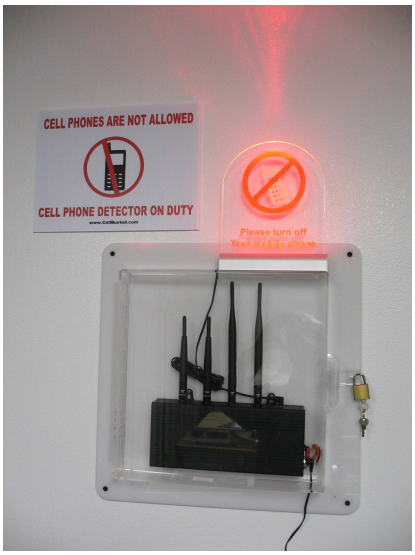
COVERT STYLE OF "AIR FRESHENER" MODEL 710

This unit is "OFFICE FRIENDLY" and wall mounts or sits on the desk in your conference/ board room environment. Comes with AC power and alkaline battery operation for portable use or where no power outlet is available.

OVERT AND 'UNFRIENDLY' <u>POLICY-ENFORCEMENT</u> TYPE:



Model 810 on **Standby**



Activated

MODEL 810 WITH HIGH DETERRENT KIT IN "STANDBY" AND "ACTIVATED" MODES

This model comes with the flashing LED illuminated sign stating "Cell Phones Are NOT Allowed In This Area" which informs the hearing-impaired (for ADA compliance) and also is good for quiet environments) churches, libraries, military conferences, etc. Choose this type when placing it at the ENTRANCE to a secure facility for overt policy enforcement alerting. The obvious nature of it helps your security policy to succeed.

This unit is available with **Silent Remote Alerting** features, so call to discuss them first.
This unit is also available with **LAN Networking** to alert to your computers desktop; call to discuss this.