How to Block Out Listening Devices

by Kevin D. Murray, CPP, CISM, CFE, CDPSE

You are probably here because you feel your privacy has been invaded. Welcome, you are not alone. Many people feel this way. With the proliferation of inexpensive and easily obtainable eavesdropping devices privacy is harder to achieve now than ever before in history.

In this article we will just focus on **audio** eavesdropping devices. If you are more concerned about **video** surveillance devices we have an informative article[1] and a course which can help you detect spycams yourself.[2] We will discuss how to block out listening devices a bit later; just after how to find eavesdropping devices.

The right to privacy is written into the constitutions of over 150 countries.[3] It has a definition in law as well. Simply put, one's personal matters should not be publicized or disclosed. In 1890 jurist Louis Brandeis mentioned it in a legal paper as *"the right to be let alone."*

The types of listening devices we will cover here are audio surveillance devices, commonly called bugs. These are the most common listening devices:

- Anything that transmits audio wirelessly at radio frequencies. Examples include: FM, digital, Bluetooth, or Wi-Fi wireless microphones, and of course cell phones.
- Anything that records sound for later listening. Examples include a variety of tape, digital, or cloud storage recorders, and of course cell phones.
- Any other thing with a microphone which moves what it hears to some other location. Examples include: smart devices (or smart assistants), and other Internet of Things gadgets.

Let's start by answering some of the common questions people have about listening devices.

Is it illegal to use a listening device?

Electronic eavesdropping without a court order in the United States is generally considered to be illegal. Some of the exceptions to the rule include:

- If you are a party to a conversation being recorded in a one-party consent state.[4] (Thirty-eight (38) states and the District of Columbia.)

Spy Pens can record or transmit – audio and video

[1] https://counterespionage.com/spy-camera-detectors/

[2] https://counterespionage.com/what-is-tscm/spycam-detection/

[3] https://en.wikipedia.org/wiki/Right_to_privacy

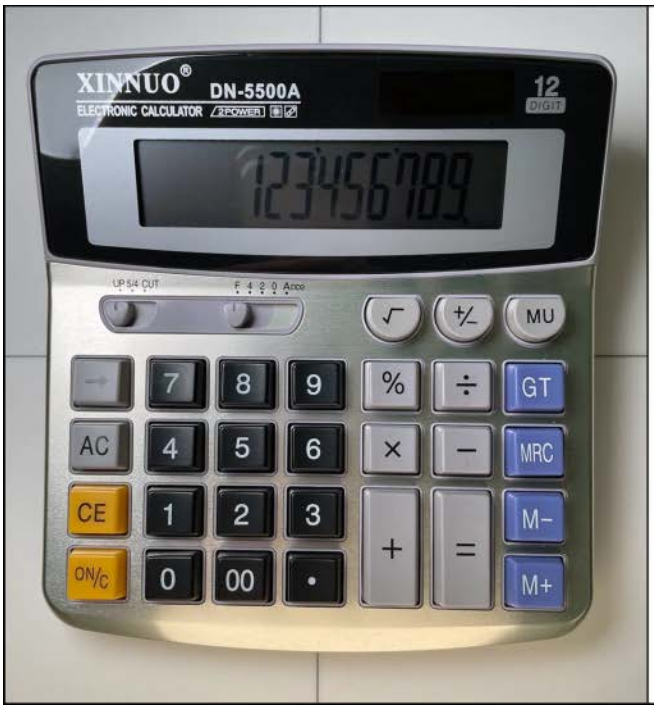
[4] https://www.rcfp.org/reporters-recording-guide/

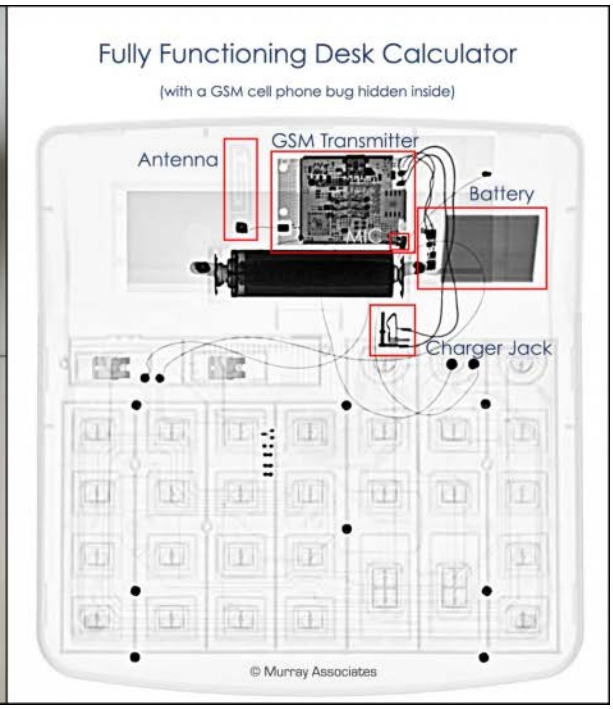
How to Block Out Listening Devices

by Kevin D. Murray, CPP, CISM, CFE, CDPSE

- In some states the concept of covertly listening exemption is referred to as, *"in the ordinary course of business,"* or the *"extension phone exemption."* This covers common carriers who need to monitor transmission quality, employee monitoring "for quality assurance," and legitimate investigative purposes. The concept has also been expanded beyond actual business situations. A parent eavesdropping on their child is one example.[5]

- The Inter-spousal wiretapping immunity exemption is based on the theory that spouses can't testify against each other. This is an old and iffy concept. In recent years, many courts have determined this exemption is no longer acceptable.





By the way, if you are thinking of taking advantage of an exemption, don't. Laws change and courts interpret rules of law on a case-by-case basis. This article is not to be taken as legal advice. Consult your attorney first if you think you have a good reason to use an electronic eavesdropping device, or other means of technical surveillance.

Do smart devices listen to your conversations?

Sure, it is what makes them smart.

The questions you should really be asking, (and what you really need to know) is…

[5] https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=3672&context=penn_law_review

How to Block Out Listening Devices

by Kevin D. Murray, CPP, CISM, CFE, CDPSE

- When do they listen?
- Where does your voice go when they listen?
- What is done with what they hear?
- How long is your voice retained?
- What access do company employees, strangers, or law enforcement have?

There is no simple answer. Each type of device will come with a different set of answers.

News reports about smart device security fails are plentiful. A few years ago it was discovered that Amazon's Alexa was sending audio of a private conversation to one of the victim's contacts.[6] Now, all three major voice assistants are facing a lawsuit for spying.[7]

Tip #1:

Assume all smart devices have microphones and they are continually listening. Assume their controlling software is not perfect, makes mistakes, and is vulnerable to hacking. You will need to unplug smart devices when you want a greater assurance of privacy.

How do you stop smart devices from spying on you?

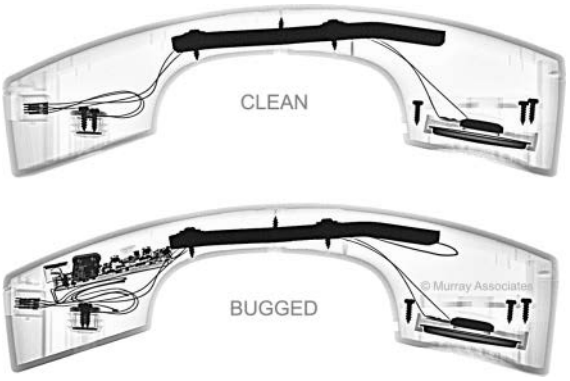
Smart devices are listening devices. In theory, they should only activate when they hear their name being called. The reality is there is no way of telling if they are behaving properly. Just try saying, "a city," "hey Jerry," "hey, seriously," "that's scary" near an Apple HomePod.

Tip #2:

If you don't feel comfortable having a smart device in your home, don't have one. That being said, they are very useful, so controlling them is the next best solution. During times you want privacy from these eavesdropping minions you will need to activate their microphone mute button. If your device doesn't have a mute button, you will just have to unplug it.

How can I tell if my neighbor has a listening device?

Your first clue will likely be them tipping their hand. Remember the taunt, "I know something you don't know," from being a kid. Obtaining confidential information can instill a feeling of power and superiority, but this only works if others know you have it. Thus, amateur eavesdroppers rarely keep their mouths shut.



Tip #3:

When a neighbor mentions things they shouldn't have knowledge of, trust your instincts, be suspicious. Read our article *Eavesdropping Snoops – The Average*

[6] https://www.cnet.com/home/smart-home/alexa-sent-private-audio-to-a-random-contact-portland-family-says/

[7] https://techstory.in/alexa-siri-google-assistant-being-sued-for-spying-on-users/

How to Block Out Listening Devices

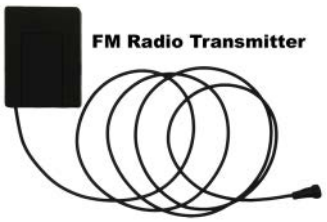
by Kevin D. Murray, CPP, CISM, CFE, CDPSE

Person's Guide to Stopping Them.[8] It contains time-tested advice which can solve your concerns without having to spend a penny.

Can listening devices be detected?

Generally speaking, they can be detected. While there are a few esoteric exceptions the types of devices the average person is likely to encounter, all are detectable. It is just a matter of combining a few detection techniques, with some knowledge of what types of devices might be used to eavesdrop on you.

Start with what made you suspicious in the first place. It was probably someone who knew something they should not have known. Just coincidence? Check.



One easy test is to make pretend phone calls from various rooms in your house. Say something interesting that would cause your eavesdropping suspect to say or do something in reaction to hearing it.

If their reaction is quick they may be listening—*in real-time*—using a radio transmitter[9] or hidden cell phone. Delayed reactions may indicated a hidden voice recorder.[10] Either way, you have narrowed your search to a particular room or area, and you have an idea of what type of device you might find. Now that you know how testing can help you, think up additional tests to cover other situations.

Conduct your tests several times. Once you have elicited three or more positive reactions you will know for certain it is audio eavesdropping and not just coincidence.

Next step… You need to identify the types of bugging devices amateur eavesdroppers use. These searches on Amazon,[11] and eBay[12] are an instant education.

Tip #4:

Instead of blocking a listening device, finding it should be your first choice. Once you do that you can remove it, or if you want to leave it in place knowing where it is makes blocking it easier. Once blocked the eavesdropper may return to fix it and you can catch them using *your* hidden camera.

Avoid buying bug detection gadgets. They often give false positive readings, and they are not made to find all types of listening devices, such as voice recorders. Worse, you may be left with a false sense of

[8] https://counterespionage.com/eavesdropping-snoops/

[9] https://www.alibaba.com/product-detail/Wireless-9V-Mini-FM-Transmitter-Module_60753863858.html

[10] https://www.youtube.com/watch?v=TymehaG_DBQ&t=1s

[11] https://www.amazon.com/s?k=listening+devices+for+spying&crid=2FS8ORCZT30SU&sprefix=listening+device%2Caps%2C168&ref=nb_sb_ss_ts-doa-p_1_16

[12] https://www.ebay.com/sch/i.html?_from=R40&_trksid=p2380057.m570.l1311&_nkw=listening+device+spy&_sacat=0

How to Block Out Listening Devices

by Kevin D. Murray, CPP, CISM, CFE, CDPSE

security if nothing is found. Grab a good flashlight instead. Conduct a physical search of the area you suspect is being bugged. Be methodical. Closely examine everything you can. Bugs can be well hidden and disguised, but they are not invisible.

Of course, if you are not qualified to take an item apart, like an electrical outlet, don't. Get someone who is qualified to help you.

If you then want to block out (instead of remove) the listening device you have several options…

- Place something nearby which will sound louder to the bug than room conversations. A radio or fan is an easy fix. A better fix for walls that are shared with neighbors, and sound migration to other rooms, are acoustical noise generators.[13]
- If battery operated, replace the batteries with dead batteries.
- If mains powered, unplug it.
- One other solution you may see being sold is the ultrasonic microphone jammer. Read *Do Ultrasonic Microphone Jammers Work?*[14] before you purchase one.

There is no 100% when discussing security and privacy. It is the age old question of, "How high do we build the wall great leader?" The answer, "Just high enough to keep them out!"

What you have learned here will help you build your wall. Our advice will help you detect and deter amateur eavesdroppers. If your concerns involve corporate espionage please contact us[15] directly for professional assistance.

Kevin D. Murray CPP, CISM, CFE, CDPSE is a business counterespionage consultant and TSCM specialist with over four decades of experience.

Murray Associates[16] is an independent security consulting firm, providing eavesdropping detection and counterespionage services to business, government and at-risk individuals.

Headquartered in the New York metropolitan area, a Murray Associates team can assist you quickly, anywhere in the United States, and internationally.

[13] https://www.google.com/search?client=firefox-b-1-d&q=acoustical+noise+generators

[14] https://counterespionage.com/ultrasonic-microphone-jammers/

[15] https://counterespionage.com/contact-murray-associates-tscm/

[16] https://counterespionage.com/about-murray-associates/electronic-eavesdropping-detection/