TSCM Bug Sweeps... When and When Not To - Part I

by Kevin D. Murray, CPP, CISM, CFE

The following advice is specifically meant for:

- Private Investigators,
- Security Directors,
- Security Consultants,
- and new TSCM practitioners.

Technical Surveillance Countermeasures (TSCM), or a bug sweep, is an analysis of an area to detect illegal covert electronic surveillance. In addition to listening devices, sweeps also take into account optical, data, and GPS tracking devices.

Part I - What *to do* when you are contacted for a TSCM bug sweep.

Let's take a typical case involving a private individual first...

Someone contacts you to *"find the bug."* They are sure they are being bugged by a: significant other, landlord, neighbor, or the amorphous, *"**They** know my every thought and move."* What do you do? Is a bug sweep really the best first step?

Probably not.

Step 1. Make sure they are not contacting you from the area they fear is bugged.

Step 2. Can you do some good?

Evaluate the situation. Is there a suspect. Is there a plausible motive?

If you hear, *"It has been happening for years. They know everything,"* your efforts are not likely to help. Avoid accepting these cases unless referred to you by a responsible party (family, legal counsel or doctor) who feels the effort is worthwhile to provide peace of mind.

Step 3. Plan your investigation.

Assuming you accept the case, start by collecting the evidence to date. Does the evidence make sense? Is it possible the client planted a bug for you to find, so it could be blamed on a third party?

Ask your client what they would like see as the outcome of their case. Do they want the snoop to permanently stop the illegal eavesdropping and/or GPS tracking? Is so, hold off on an immediate bug sweep. Even if you find a device, all you have is a hand full of hardware. You also have an alerted snoop who is free to strike again, next time more covertly. If the situation is not ongoing, a sweep to clear out previously planted devices might be warranted.

Step 4. Tie the criminal to the crime.

The quickest way to stop a snoop is by stomping on their toes with a lawsuit.

Tie the criminal to the crime.

Work with your client to document the circumstantial evidence of electronic surveillance noticed so far. A sting operation can help fortify this evidence.

Have your client selectively drop bits of specific information, or in the case of GPS tracking, visits to unique locations. This activity should be

TSCM Bug Sweeps... When and When Not To - Part I

by Kevin D. Murray, CPP, CISM, CFE

crafted to trigger a reaction by the snoop, a reaction which would only happen if they were conducting electronic surveillance.

Log dates, times, the bait information floated, and reactions observed, with those dates and times. Don't stop after the first positive reaction. You want to log at least three or more reactions. Doing this will counter any *coincidence defense* the snoop may raise later.

Step 5. Bring your findings to an attorney.

Work with an attorney to determine the best way to proceed. Is there enough evidence? Should the case be filed as criminal or civil, or both?

Let the attorney determine when a bug sweep should be conducted and who should do it. You may be capable, but will your qualifications hold up in court? Success may hinge on having the testimony of an independent specialist.

Step 6. Conducting a TSCM bug sweep.

Partner with a competent specialist. You or the attorney may already have someone you know and trust. If so, great. If not, conduct a search using terms like "*Advanced TSCM.*"

Once you have found specialists to vet, ask plenty of questions. If you are not sure of what to ask, search *TSCM compare* (skip the paid ads) for a list of questions.

Qualify your specialist with questions, but be sure to note their professionalism, too. Their presentation and demeanor will reflect on you, and the judge.

A typical case involving a business client...

Word about something has leaked out. *"Check everything,"* barks the boss. What do you do? Is an inspection for bugs and wiretaps the best first step?

A TSCM Inspection is the best first step, but advise the client that checking everything may not be the best way to proceed.

Step 1. Make sure they are not contacting you from the area they fear is bugged.

Step 2. Can you do some good?

Yes!

Although a vast majority of leaks are caused by employees with big mouths and sloppy security habits, an inspection for surveillance devices is an important first step. Electronic spying has to be ruled out *before* investigating and accusing people.

Of all business espionage tricks, electronic surveillance is one of the most popular, and the easiest to discover.

Step 3. Plan your investigation.

Calm your client. Ask: what raised their suspicions; where was the missing information discussed or stored. Ask for a *prioritized* list of sensitive areas as it is rarely necessary to "check everything." Working your way down this list will

TSCM Bug Sweeps… When and When Not To - Part I

by Kevin D. Murray, CPP, CISM, CFE

conserve your client's budget and focus your, or your specialist's, talents.

Also, plan a course of action should a device be found. This is important. Without a plan, revealing a surveillance device will come as an emotional shock to your client. Snap judgement decisions made under these conditions are usually poor decisions.

Partner with a specialist. As good as you may be, the average security practitioner is no match against a concerted business espionage effort. Besides, you will be busy following up on your specialist's recommendations for additional investigation and security implementations.

Step 4. Conduct the investigation.

Although the chances of finding an *active* surveillance device are increased during work hours, a properly equipped specialist will not be impeded by conducting the inspection during off-hours. In fact, there are some definite advantages to an off-hours inspection:

- No disruption of business.
- No alerting employees – one of whom may be in on the spying.
- A better opportunity to evaluate current information security effectiveness.

Work your way down the priority list of areas. At some point you will be able to say, *"If nothing was found at the high sensitivity levels, lower level snooping is unlikely."*

If a device is found, keep searching. Sometimes multiple devices are planted, with some *planted to be found,* hoping the discovery will end the search early.

Expand the search down the list as necessary.

If a device is found:

- Do not disturb the device. It is evidence.
- Do not alert the eavesdropper by talking.
- Secure the area. It is a crime scene. (Use a non-alerting excuse.)
- Document your evidence. Make notes. Take photos.
- Only notify people who have a real need-to-know.
- Tell all persons involved to keep it confidential.
- If you are not a TSCM practitioner, contact an independent information security consultant who specializes in Technical Surveillance Countermeasures (TSCM).
- Make all communications from a safe area, using a safe phone, of course.

Step 5. Solve the investigation.

It may be possible to determine who planted the electronic surveillance device with counter-surveillance.

- Watch the device with a covert video camera. See who comes to change the batteries, if any.

TSCM Bug Sweeps... When and When Not To - Part I

by Kevin D. Murray, CPP, CISM, CFE

- Place something which generates noise near it. See who comes to relocate the device.
- Feeding the device false information might help ferret out the spy as well.

Step 6. What to do with positive findings?

This is a highly debatable question. Some say, contact law enforcement. Some say, bring your findings to the client's legal counsel. Some private detective statutes prohibit reporting to anyone except your client.

Realistically, your client will want to control things from this point on. Be ready to advise them, but don't count on being asked. If some cases go to court, most go under the carpet.

In Part II, we'll discuss how to help your current business clients.

###

About the Author

Kevin D. Murray CPP, CISM, CFE is a technical information security consultant and TSCM specialist with over four decades of experience.

Murray Associates is an independent security consulting firm which provides 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.