## Common Sense Security

**By Sheila O'Donnell**

As our movements have become stronger and more sophisticated, the techniques of the state, corporations, and right-wing groups have also become more sophisticated. We have seen government agents, corporate security and right-wing intelligence networks share information as well as an ideology. For instance, the FBI's COINTELPRO operations targeted dissidents in America in the 1960s and 1970s. Caution and common sense security measures in the face of the concerted efforts to stop us are therefore both prudent and necessary.

Spend a few minutes to assess your work from a security point of view: understand your vulnerabilities; assess your allies and your adversaries as objectively as possible; do not underestimate the opposition. Try to assess your organizational and personal strengths and weaknesses. Do not take chances. Plan for the worst; work and hope for the best.

Here are some specific suggestions for protecting yourself and your projects:

### Office

- Never leave the only copy of a document or list behind; take a minute to duplicate an important document and keep the duplicate in a safe place off-site.
- Keep mailing and donor lists and personal phone books out of sight. Always maintain a duplicate at a different location; update it frequently.
- Know your printer if you are about to publish and know your mailing house if you contract for distribution. The loss of camera-ready copy or a change in text could feel like a disaster.
- Back up and store important computer disks off-site. Sensitive data and membership lists should be kept under lock and key. Do not leave sensitive files on the hard disk; use floppies, back them up, and store the disks in secure spots. Use an encryption program to protect your data.
- Know the background of anyone you are trusting to work on any part of a project that is sensitive. Projects have been bungled because an untrustworthy person has purposefully intervened or inadvertently screwed up.
- Don't hire a stranger as a messenger. Your message might not arrive or could arrive after being duplicated for an unintended party.
- Sweeps for electronic surveillance are only effective for the time they are being done, and are only effective as they are being done if you are sure of the person(s) doing the sweep. Sweeps tend to be expensive because one must sweep a large area to be effective. Many experts contend that the most sophisticated federal government and

private agency taps cannot be detected.
- Keep a camera handy at all times.

### Trash

- What you consider trash could be a real treasure to someone looking for information about you or your projects. Don't throw information out in your trash. Garbology has become a tactic because it is so useful.
- Keep a "Burn file" in a secure place and occasionally burn it or use a shredder. Make sure you shredder creates confetti because strips can easily be reconstructed with a little patience.

### Telephone

- Do not list your address with your phone number in the directories. Consider having yourself unlisted.
- If you receive threatening calls on your answering machine, immediately remove and save the tape.
- Never respond to a query over the telephone from an unknown person--lottery tickets, fabulous prizes, jury questionnaires, etc. notwithstanding. Ask for a telephone number and call the party back considerably later or the following day. Check the phone book to see if the phone number they gave you is legitimate. Check it out. Do the same if a reporter calls.
- Never say anything you don't want to hear repeated where there is any possibility of being recorded or overheard. Don't say anything on the phone you don't want to hear in open court.
- Don't talk in code on the telephone. If you are being tapped and the transcript is used against you in court, the coded conversation can be alleged to mean anything by government code "experts."
- Don't gossip about sensitive people or projects on the telephone. All information that can make an outsider "in the know" about you and your projects is valuable and makes everyone vulnerable.
- Keep a pad and pen next to the telephone. Jot down details of threatening or suspicious calls immediately. Note the time, date and keep a file.
- Don't waste time worrying about phone taps or imagining that strange clicks or hums or other noises indicate a phone tap. Many taps are virtually impossible to detect. Trust your instincts. If you think your phone is tapped, act accordingly.

### Mail

- Get a mail box through the United States Post Office or a private concern. Be aware that the Post Office will give your street address to inquirers under certain circumstances.
- If you receive a threatening letter, handle it as little as possible. Put both the letter and the envelope in a plastic bag or file folder. Give the original to the police only if they agree to fingerprint it. If not, give them a copy because you may wish to have your own expert examine it.

### Automobiles

- Keep your automobile clean so you can see if there is an addition or loss.
- Put no bumper stickers on your car which identify you as an organizer. Make your car look ordinary.
- Put your literature in the trunk or in a closed box.
- Keep your car locked at all times.

### Police

- Report any incidents to the local police and ask for protection if you feel it is warranted.
- Report threats or harassment to your local police. Demand that they take a report and protect you if that is necessary. Talk to the press and report the police response as well

- Talk to Action
- Open The Government
- Building Human Rights
- Stop Spying
- Other Allies in Activism and Research



Updates and Corrections

as the incident(s).
- Report thefts of materials from your office or home to the police; these are criminal acts.

### Under Surveillance?

- Brief your membership on known or suspected surveillance. Be scrupulous with documentation. Do not dismiss complaints as paranoia without careful investigation. The opposition can and frequently does have informants join organizations to learn about methods and strategy.
- Discuss incidents with colleagues, family, and membership. Call the press if you have information about surveillance or harassment. Discussion makes the secret dirty work of the intelligence agencies and private spies easier to spot.
- If you wish to have a private conversation, leave your home or office and take a walk or go somewhere very public and notice who can hear you.
- If you know a secret, keep it to yourself. As the World War II poster warned: loose lips sink ships.
- Photograph the person(s) following you or have a friend do so. Use caution. If someone is overtly following you or surveilling you, she or he is trying to frighten you. Openly photographing them makes them uncomfortable. If you are covertly being followed, have a friend covertly photograph them.
- If you are being followed, get the license plate number and state. Try to get a description of the driver and the car as well as passengers. Notice anything different about the car.
- If you are followed or feel threatened, call a friend; don't "tough it out" alone. "They" are trying to frighten you. It is frightening to have someone threatening your freedom.
- Debrief yourself immediately after each incident. Write details down: time, date, occasion, incident, characteristics of the person(s), impressions, anything odd about the situation.
- Keep a "Weirdo" file with detailed notes about unsettling situations and see if a pattern emerges.

### Break-Ins

- Check with knowledgeable people in your area about alarm systems, dogs, surveillance cameras, motion sensitive lights, dead bolt locks, and traditional security measures to protect against break-ins.

### Visits From the FBI

- Don't talk to the FBI or any government investigator without your attorney present. Get the names and addresses of the agents and tell them you will have your attorney contact them to set up a meeting. If you have an attorney, give her or him the name and phone number. Under any circumstance, get the agents' names and addresses. Information gleaned from a conversation can be used against you and your co-workers. The agents' report of even an innocuous conversation could "put words in your mouth" that you never uttered or your words could be distorted or made up if you don't have your attorney present.
- Call the National Lawyers Guild, American Civil Liberties Union, or other sympathetic legal organizations if you need assistance locating a reliable attorney in your area.
- The FBI rarely sets up interviews with counsel present. Often when the demand is made to have the interview with counsel, the FBI loses overt interest.
- Don't invite agents into your home. Speak with the agents outside. Once inside, they glean information about your perspective and lifestyle.
- Don't let agents threaten you or talk you into having a short, personal conversation without your lawyer. Don't let them intimidate or trick you into talking. If the FBI wants to empanel a Grand Jury, a private talk with you will not change the strategy of the FBI. Don't try to outwit the FBI; your arrogance could get you or others in serious trouble.
- FBI agents sometimes try to trick you into giving information "to help a friend." Don't fall for it; meet with the agents in the presence of your attorney and then you can help

your friend.
- Lying to the FBI is a criminal act. The best way to avoid criminal charges is to say nothing.
- Any information you give the FBI can and will be used against you.
- Write for your government files under the Freedom of Information Act and keep writing to the agencies until they give you all the documents filed under your name.
- Don't let the agents intimidate you. What if they do know where you live or work and what you do? We have a constitutional right to lawful dissent. You are not required to speak with the FBI. They intend to frighten you; don't let them.
- Do not overlook the fact that government agencies sometimes share information within the government and with the private sector, particularly right-wing organizations. This has been documented.

### Remember

If you feel you are being surveilled, your phones tapped, or that you are being followed, the best overall advice is to trust your instincts. If you feel something is wrong, trust the feeling. Your instincts are usually right. Most of us recall the times when we "felt something was wrong" or we "knew better but did it anyway."

Talk to colleagues and make yourself as secure as you can. Experts claim that people who resist get away from attackers more often than those who do not. The same logic applies to keeping outsiders out of your business; it is a more subtle form of attack.

Trust your instincts and resist when possible. One of the biggest blocks to resistance is the failure to recognize that we are under attack. None of this advice is intended to frighten but to create an awareness of the problems. A knowledge of the strategies and tactics of your adversaries will strengthen your movement. Cover yourself; it's a tough world out there.

### Suggested Readings

Caignon, Denise and Gail Groves. Her Wits About Her: Self Defense Success Stories by Women. New York, 1987.

Churchill, Ward and Jim Vander Wall. Agents of Repression: The FBI's Secret Wars Against the Black Panther Party and the American Indian Movement. Boston: South End Press, 1988.

Donner, Frank J. The Age of Surveillance. New York: Random House, 1981.

Gelbspan, Ross. Break-ins, Death Threats and the FBI: The Covert War Against the Central America Movement. Boston: South End Press, 1991.

Glick, Brian. War at Home: Covert Action Against US Activists and What We can Do About It. Boston: South End Press, 1989.





Political Research Associates • 1310 Broadway, Suite 201 • Somerville, MA 02144
Voice: 617.666.5300 • Fax: 617.666.6622 • pra@publiceye.org