centerforconstitutionalrights

on the front lines for social justice

Table of Contents

Introduction

Federal law enforcement agencies like the Federal Bureau of Investigation (FBI) have a dark history of targeting radical and progressive movements. Some of the dirty tricks they use against these movements include: infiltration of organizations to discredit and disrupt their operations; campaigns of misinformation and false stories in the media; forgery of correspondence; fabrication of evidence; and the use of grand jury subpoenas to intimidate activists. Today's activist must know and understand the threat posed by federal law enforcement agents and their tactics as well as several key security practices that offer the best protection.

Federal agents have many tools at their disposal to target activists. While it is important to know and understand these tools and tactics, it is of critical importance that you resist any paranoia of government surveillance or fear of infiltration, which will only serve to paralyze you or your organization in your quest for social change. If fear of government repression prevents you from organizing, the agents of repression will have won without even trying.

The Center for Constitutional Rights (CCR) created If an Agent Knocks to provide advice to activists likely to be targeted by FBI agents or other federal investigators. Since its original release in 1989, If an Agent Knocks has been widely circulated in progressive activist communities across the country. This guide includes both the timeless advice included in the original version and extensive updates to reflect the current state of the law and law enforcement tools. This updated edition also includes a comprehensive discussion of today's technology, including cell phones, e-mail and Web browsing. This guide should be seen as a resource for the information needed to protect yourself and other activists from government investigation and to empower you to continue the struggle.

We have attempted to provide answers to a broad range of ques-

tions for the many scenarios that one can encounter as an activist. We hope individuals and groups use this pamphlet to develop and prepare practical responses – if an agent knocks at your door.

This publication consistently emphasizes that professional legal advice should be sought in all cases. The Center for Constitutional Rights does not have the capacity to provide individual criminal representation.

Each state has bar associations that should be able to make attorney referrals, some of whom may provide pro-bono services. If there is a chapter of the National Lawyers Guild (www.nlg.org) in your city, they are often able to make referrals to attorneys who are experienced in dealing with the issues outlined in this booklet.

Visits & Searches

If I Am Approached or Called by a Law Enforcement Agent, Do I Have to Talk?

This is the most important piece of information in this booklet: you have the right to remain silent, and it is usually the best idea to do so. The Fifth Amendment of the United States Constitution protects you from being forced to reveal self-incriminating information to law enforcement.

This is easier to say than to do. Agents are trained investigators: they have learned the power of persuasion and the ability to make a person feel scared, guilty or impolite for refusing their requests for information. An agent may suggest that any unwillingness to speak with her/him means you must have something to hide. S/he may suggest s/he only wants you to answer a few questions and then s/he will leave you alone. The agent may threaten to get a warrant.

Don't be intimidated or manipulated by an agent's threats or assurances. It is always best to not talk without an attorney present. If you do talk, anything you say can be used against you and others. Even if you tell the whole truth, if the agent doesn't believe you, s/he can threaten to charge you with lying to a federal officer – which is a real crime.

Clearly convey your intention to remain silent. Say "I'm not talking to you," or "I'd like to talk to my lawyer before I say anything to you." You can also say, "I have nothing to say to you. I will talk to my lawyer and have her/him contact you." You should ask the agent for a business card and say you will have your lawyer contact them. This should end the questioning.

The one exception to this rule is if you are in a state that has a "stop-and-identify" statute. All states require you to produce a drivers license if you are pulled

over while driving an automobile, and the Supreme Court has held that laws that require you to state basic identifying information, such as your name and address, are not considered incriminating and that law enforcement may demand such information you. They may only demand that information from you, however, if you are in a state that has a stop-and-identify statute. An activist attorney in your state should be able to tell you if your state has a stop-and-identify statute.

The same basic rules apply if an agent calls on the phone. You do not have to speak to any agent who spontaneously calls you. Agents will often say that you are not part of any investigation. This may not be the truth. Tell anyone who identifies themselves as law enforcement that you will have your lawyer call them back – and then stop talking to them.

If possible, get the agent's name, telephone number and agency. This should be on her/his business card, or s/he should be willing to provide this information.
As soon as the agent leaves or hangs up, try to write down as many details about the interaction as you can. This information will be useful to a lawyer and to others who have been contacted by law enforcement. Try to write down the name of the agent(s) and her/his physical description; the type of car the agent was driving; the questions asked and comments made during the interaction; the date, time and location of the encounter; and the contact information of any witnesses.

The best course of action is usually to get a lawyer involved. A lawyer can offer advice on how to proceed while protecting your rights. A lawyer can talk to the agent; find out what the investigation is about; try to set limitations on the subject matter of any questioning; and be present to advise and protect you if you are questioned. Sometimes a call from a lawyer is all it takes to get an agent to back off.

With the advice of a lawyer, you may consider publicizing the encounter to others who may be affected by an investigation. If activists know that there is an investigation, they can be more vigilant in protecting their rights. Organizing and public pressure can expose and limit intimidation and fishing expeditions.

1. At the time of publishing, the following states have some version of a stop-and-identify statute: Alabama, Arizona, Arkansas, Colorado, Delaware, Florida, Georgia, Illinois, Indiana, Kansas, Louisiana, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Mexico, New York, North Dakota, Ohio, Rhode Island, Utah, Vermont and Wisconsin.

What Are The Consequences If I Do Talk?

A situation may arise where you feel it is advisable to talk to an agent. Perhaps you have been the victim of a crime or you are a witness to civil rights violations being prosecuted by the federal government.

Even in those circumstances, you should have a lawyer present. A lawyer can make sure your rights are protected while you provide only necessary information relevant to a specific incident. They may be able to help you avoid a witness' appearance before a grand jury or control the circumstances of the appearance so that no one's rights are jeopardized.

If you do decide to answer questions, be aware that lying to a government official is a crime. In fact, one of the most important reasons to not talk to an agent is this crime. A standard federal law enforcement tactic is to discover as much information as possible about a suspect or merely a person of interest to the government. Federal law enforcement agents will then approach that person at an otherwise ordinary time, such as during dinner or at the bus stop, and ask the person questions to which they already know the answers.

For example, an agent might ask if you know a person (whom they know that you know) or might ask if you were at an event (at which they know you were in attendance). If you instinctively say "No," that is a federal felony punishable with five to eight years in prison. The most daunting aspect of this investigative tactic is that many individuals will instinctively answer no to a question because they are scared or nervous. This tactic is used extensively by federal agents in all types of investigations and has been used recently to target and turn activists into informants against their former associates.

Lying to a federal officer is a federal offense and only applies to questions asked by federal agents. Be aware, however, that some local and state agents, such as members of a city's Joint Terrorism Task Force, are also considered "federal" agents. As well, some states have similar crimes regarding lying to a state officer. The safest choice is not to talk to law enforcement.

If you start answering questions, you can refuse to continue answering questions at any time.

Search Warrants

A search warrant is a court order authorizing law enforcement to search a specified location and seize evidence.

The Fourth Amendment protects people against unreasonable searches. Unless an exception applies, law enforcement agents are required to obtain a search warrant to conduct a search. Search warrants must be supported by probable cause, with facts sworn to by the officer applying for the warrant. A search warrant should be specific to the area to be searched and the object(s) to be searched for. It should be signed by a judge, be dated with a recent date (within a couple of weeks) and state the correct address for the location.

Probable cause means that facts must exist to establish that evidence of a crime will probably be found in the area to be searched. Probable cause must be based on facts – hunches are not enough.

Armed with a search warrant, law enforcement agents have the right to search your property. If you do not grant them access, they will likely use force to execute the search.

Know Their Tools

What If An Agent Asks to Search My Home, Apartment or Office?

Never allow law enforcement to search your person or property without a warrant. Law enforcement agents are required to have a warrant to search your property except for certain limited circumstances. You are only legally required to allow law enforcement agents into your home, office or other private space if they have a warrant.

Agents may search your house without a warrant if you allow them to, and they are trained to seek your consent to warrantless searches. Be careful of questions that are designed to elicit your consent to search. These questions may be as innocuous as “Do you mind if I come in?” Simply allowing an agent into your home may be construed as consent to search the whole place.

Legally, the best answer to a request to search is “I do not consent to a search.” Say it loudly and proudly so any witnesses can hear.

What If I'm Not Around and an Agent Asks My Roommate to Search My Property?

A roommate can consent to a search of common, shared space and to her/his own space. A roommate cannot consent to search of another person's private space in a shared house or apartment. In other words, a roommate could consent to a search of your kitchen, living room or shared bathroom, but not your private bedroom, unless you share it with her/him or it is used as a common space in some way.

Spouses can consent to the search of their partner's private rooms because they are considered to have shared authority over all space in the house. Similarly, parents can consent to a search of their children's private space. In sum, if you share a bedroom with a roommate or partner, they can consent to a search of that space.

To protect against unwanted searches, make sure private space remains private. If you allow roommates to have mutual access and control over your private space, they can consent to a search of that space. Tell roommates, office mates and anyone with whom you share space to never consent to searches of any space, especially your private space.

Can Agents Search My Trash?

Once you have placed your trash outside your house, agents can search it without a warrant or any other legal restraint. Courts have found that you have no privacy interest in your trash because you are surrendering it to the general public. Shred or otherwise destroy any and all sensitive documents before disposing of them.

What If an Agent Threatens to Get a Warrant or Grand Jury Subpoena Unless I Talk or Consent to a Search?

Don't be intimidated by an agent's threats to get a warrant or subpoena. This is one of the oldest tricks in the book. If it were so easy for the agent to get a warrant or subpoena, s/he wouldn't have wasted time trying to get your voluntary cooperation. Again, simply state that you will not consent to any search and that you will not talk without a lawyer present.

What If an Agent Claims to Have a Search Warrant?

If an agent claims to have a warrant, ask to see it. It should look similar to the sample search warrant featured here and must be signed by a judge to be valid. A search warrant should be specific as to the area to be searched and the object(s) to search for. Do not consent to an agent searching any areas not specifically included in a search warrant.

Just because an agent has a search warrant doesn't mean you have to answer any questions. Maintain your right to silence during the search – clearly state that intention if you are asked any questions.

What Rights Do I Have to Keep Agents From Searching My Car?

Law enforcement has extremely broad power to conduct warrantless searches of cars. If an agent has probable cause to believe that a car contains evidence of a crime, the agent may, without a warrant, search the vehicle and any container inside the vehicle that is large enough to contain the item for which s/he had probable cause to search. For example, if an agent has probable cause to believe you stole a large television, s/he can search the trunk of the car but not the glove box or a small toolbox in the trunk. If s/he only has probable cause to search a container recently placed in the car, s/he can only search that container.

If you are arrested and your car is impounded, law enforcement is allowed to perform a warrantless inventory search. This basically means the police may search your car for the purpose of cataloging what is inside, but they may use anything they find against you for any reason. Inventory searches must follow local established procedures, and the police may not use an inventory search as pretext for performing a warrantless search.

What Should I Do If My Office or Home Is Broken Into and I Suspect That the Motive Was Intelligence Gathering?

If your home or office is broken into, or if threats have been made against you, your organization or someone you work with, share this information with everyone affected and take immediate steps to increase personal and office security. Contact a lawyer immediately.

"Sneak and Peek" Searches

"Sneak and peek" searches allow the government, with secret approval from a court, to conduct searches and surveillance without notifying the subject of the search. Since sneak-and-peek searches are intended to be carried out secret, they usually are conducted through breaking and entering.

Normally an agent has to go before a judge and demonstrate probable cause in order to obtain a search warrant. In the Foreign Intelligence Surveillance Court, however, agents can obtain authorization to conduct a sneak-and-peek search if they can demonstrate that the search will provide foreign intelligence information. And, foreign intelligence gathering doesn't have to be the primary reason for the search; it just has to be a significant reason for the search. This means that an agent can get authorization to search your home to gather evidence of criminal acts so long as foreign intelligence gathering is also a goal in the search.

While sneak-and-peak searches were designed for purpose of gathering foreign intelligence information, most courts have allowed evidence and information obtained from sneak-and-peek searches to be used in criminal prosecutions.

⚠ Know Their Tools

What Should I Do If Agents Show Up With an Arrest Warrant?

An arrest warrant is a tool used by police and other law enforcement agents to enter your home to make an arrest. One of the many loopholes in search warrant requirements is that once the agents are inside your home, even if they are there with only an arrest warrant, they have great leeway to conduct a search. They can search the immediate area around you without a search warrant. Law enforcement agents can even search the whole house as part of a "protective sweep" if they have a reasonable belief that a dangerous person might be present there.

If law enforcement arrives at your home (or any other space) with an arrest warrant, the best thing to do is go outside and give yourself up. If it is safe to do so, lock the door behind you. If law enforcement agents have an arrest warrant, they will arrest you. Do not give them the chance to conduct a warrantless search of your home as well.

Arrest Warrant

An arrest warrant is a court order authorizing law enforcement to arrest a specified person. Arrest warrants are signed and issued by a judge based on sworn applications from law enforcement attesting that there is probable cause that a crime has been committed and the person or people named in the warrant committed the crime.

In general, police and other law enforcement agents don't need a warrant to make an arrest. If they have probable cause to believe a crime has been committed, they can make an arrest.

There are two common exceptions to this rule. First, in most but not all states, law enforcement agents need a warrant to make an arrest for a misdemeanor that they did not witness personally. It is important to note, however, that agents can still make arrests for felonies they did not witness without an arrest warrant. Secondly, law enforcement generally needs an arrest warrant to make an arrest in your home. They can, however, make a warrantless arrest in your home if they believe there is a risk that you will destroy evidence or if they are in chasing you in hot pursuit and you duck into your or someone else's home.

⚠ Know Their Tools

What Should I Do If I Receive a Subpoena?

You should seek to quash the subpoena before the date of compliance specified on the subpoena itself, but even subpoenas that state they require immediate compliance cannot be enforced without a judge.

If someone shows up at your door and tries to serve you with a subpoena, just take it. Don't let the person in, don't answer any questions and don't consent to a search. A subpoena does not give an agent the right to take any immediate action.

Subpoenas

A subpoena is an order issued by a government authority that demands someone turn over physical evidence, such as documents, or that the person testify in court.

Subpoenas are extremely easy to obtain. They are often filed by a government employee, a court clerk and even private attorneys. A subpoena does not need to be presented to a judge before it is issued. The showing required to issue a subpoena is extremely low; a subpoena may be issued if there is any reasonable possibility that the physical evidence or testimony demanded will provide information relevant to the subject being investigated.

The ease with which subpoenas are issued makes them a powerful tool, but unlike search warrants or other government tools, they can be challenged in court prior to compliance. If you receive a subpoena, you can move to "quash" the subpoena if it is too broad or too burdensome or if it seeks legally protected materials, including materials protected by the First Amendment. Once a subpoena is quashed, the documents or testimony demanded are no longer required of the recipient.

Subpoenas are particularly dangerous because law enforcement can subpoena third parties that may have information about you. The government can subpoena other people for e-mails you have sent them. Or they can ask your e-mail provider for them. Because these third parties do not have the same interest in defeating these subpoenas that you do, and are more likely to comply with the subpoena without a fight.

⚠ Know Their Tools

What Should I Do If I Receive a Subpoena? (continued ...)

You should obtain the services of an attorney to help you quash the subpoena.

In the unlikely event that you are informed that a third party has been subpoenaed for records about you, you can move to quash that subpoena – it does not matter if a subpoena wasn't issued directly to you.

Infiltration & Human Surveillance

The use of undercover agents and informants is indispensable in investigations by modern law enforcement agencies. The ability to place undercover agents or informants in progressive movements or organizations gives law enforcement a kind of access that is otherwise nearly impossible to obtain. Infiltration is very useful to collect confidential information on the activities of private individuals and give law enforcement enough information to initiate an investigation. Undercover agents and informants can report to law enforcement on the participants, tactics and actions of movements. They can even suggest, encourage and/or participate in illegal activity in their efforts to arrest participants. Courts have generally held that public policy forbids the disclosure of an informant's name unless essential to the defense in a criminal court, so informants are rarely called upon to testify, enabling them to act with only a limited amount of responsibility or accountability.

Informants

Informants are individuals who are not employed as law enforcement agents who provide law enforcement agents with information, often in exchange for money. An informant ordinarily has previous involvement in – and more intimate knowledge of – the movement or organization that the agents are investigating.

⚠ Know Their Tools

Undercover Agents

An undercover agent is a law enforcement officer who uses an assumed name or fake identity to infiltrate a movement or organization to gather information or evidence. In political infiltration cases, an agent will typically pose as a sympathizer to a particular organization, gain the trust of its key members and then use this access to gather confidential information to pass on to the investigative agency. A secondary objective may be to lay the groundwork for a separate investigation. Undercover agents typically concoct a cover story as detailed as the assignment requires as well as a basic biography and plausible story covering past and present activities.

Know Their Tools

Cooperating Witnesses

Cooperating witnesses are similar to informants, except that cooperating witnesses usually agree to "flip" or "snitch" after being threatened with prosecution. Cooperating witnesses will testify in court in exchange for lesser charges being filed against them if there are any charges filed against them at all.

Law enforcement recruits informants and cooperating witnesses from the ranks of people already active within the movements or organizations being targeted. The government often threatens these individuals with charges carrying massive jail time, offering to not file charges in exchange for a promise to inform on others in the movement. Undercover agents, on the other hand, use false pretenses from the beginning of their association with any movement or organization.

Know Their Tools

Are There Limits on What Undercover Agents and Informants Can Do?

No specific law governs or limits law enforcement's use of undercover agents or informants, and there are no restraints on what types of crimes infiltration can be used to investigate. Unlike other countries, the use of covert practices do not require a warrant, so law enforcement officers don't need to show that the use of an undercover agent or informant is necessary for a particular investigation. The FBI's use of undercover agents and informants is governed only by loose internal guidelines established after U.S. Congressional findings in the *Final Report of the Select Committee to Study Government Operations with Respect to Intelligence Activities (1976)*.

The report exposed details about the FBI's now-infamous Counter Intelligence Program (COINTELPRO) program, in operation between 1956 and 1971, which targeted activists and organizations, including Dr. Martin Luther King, Jr. and the Black Panther Party. In response to the report, the U.S. Attorney General enacted internal guidelines for covert FBI operations that regulated both undercover agents and informants. While these guidelines were initially strong, they have been progressively weakened by several administrations. The current guidelines permit many of the invasive law enforcement practices they were originally designed to prevent. Moreover, the guidelines are not enforceable in court, so they offer only limited protection from infiltration and surveillance. In other words, if an agent gathers evidence in violations of FBI regulations, that evidence might still be used in court.

What is Entrapment?

The strongest restraint on undercover agents and informants is the requirement to avoid entrapment. Entrapment occurs when an agent or informant plants the idea to commit an offense in the mind of an individual who would not otherwise have been disposed to commit such an offense and then encourages that individual to commit the offense in order to prosecute her/him. Courts view entrapment very narrowly, and tend to give wide latitude to undercover agents or informants who suggest or encourage illegal activity. While exceptions to the entrapment defense vary from state to state, it is generally not an effective defense if the undercover agent merely suggested the commission of a crime. In many states, entrapment is not a viable defense if a jury believes someone was predisposed to commit the crime. In other states, entrapment is not

What is Entrapment? (continued ...)

a defense at all when the crime involves "causing or threatening bodily harm." For these reasons, one cannot rely on the availability of an entrapment defense.

What are the Constitutional Limits to an Agent's Power to Infiltrate?

Undercover agents or informants are generally allowed to attend public meetings, including those that take place in houses of worship. Courts have sometimes found First Amendment violations when it is determined that enforcement agents interfered with a group's ability to exercise the right to freedom of speech and association. Similarly, courts have found law enforcement in violation of the First Amendment when it gathers and publicly releases information on an activist or organization. Courts have not found First Amendment violations when law enforcement agents merely create an uncomfortable atmosphere at public meetings.

Courts have routinely found that the covert recording of conversations by undercover agents and informants does not violate the Fourth Amendment, which protects against unreasonable searches and seizures.

Courts have also found that the covert recording of conversations by undercover agents and informants does not violate the Fifth Amendment protection against self-incrimination. Similarly, if you unknowingly invite an undercover agent into your home or other private space, courts consider it "consent" to a search by that agent. If the undercover agent sees probable cause of a crime, s/he can then summon other law enforcement agents to join in the search based on the so-called consent granted to the undercover agent. Some courts have even applied the same reasoning for situations in which targets unknowingly invite an informant to enter a home.

How Can I Determine Evidence of Infiltration?

There are some helpful clues to identify an infiltrator. An undercover agent or informant may volunteer for tasks that provide access to your group's important meetings and papers, such as financial records, membership lists, minutes and confidential files. Undercover agents and informants often encourage or urge the use of violence or illegal tactics and accuse others who resist those tactics as being cowards. Similarly, undercover agents or informants often accuse others of being agents or informants, thereby diverting attention from themselves and distracting the group from its work. An undercover agent or informant may also have no obvious source of income over a period of time or have more money available than her/his job should pay.

Try to obtain information on a suspected agent or informant's background. Check with organizations in areas the suspected agent lived in the past to see if anyone can vouch for her/him. See what you can turn up on the Internet. Public records such as credit reports, voter registration and mortgages contain a wealth of information, including past and present addresses. If they are available, you might want to check listings of local police academy graduates; but, remember that the suspected person may not be using her/his real name.

A person who fits these characterizations is not necessarily an undercover agent or informant. Use caution and do not accuse someone of being an agent or informant unless you have substantial evidence against them.

What Precautions Can I Take to Protect My Organization?

Maintain a file of all suspected or confirmed experiences of surveillance and disruption. Include the date; place; time; those present; a complete description of everything that happened; and any comments explaining the context of the experience and an description of the impact the event had on the individual or organization. Hold a meeting to discuss spying and harassment, and determine if any of your members have experienced any harassment or noticed any surveillance activities that appear to be directed at the organization's activities. Review past suspicious activities or difficulties in your group, and try to determine if one or several people have been involved in many of these events.

You may try to file Freedom of Information Act (FOIA) requests for your organization from agencies such as the FBI, Department

of Homeland Security (DHS), the Bureau of Alcohol, Tobacco and Firearms and other federal agencies. File similar requests with local and state law enforcement agencies utilizing your state's freedom of information laws.
Most importantly, do not allow paranoia about infiltration paralyze your movement or organization. Paranoia can be as destructive as infiltration itself.

Electronic Surveillance

This chapter addresses the ways that agents can use telephone wiretaps, bugs and Internet surveillance in their investigations. As our lives become evermore digitized, agents are increasingly using electronic surveillance to collect information. Unfortunately, the law and the courts usually fail to keep up with the pace of technology, which often leads to unknown or diminished privacy protection for the latest technology.

A good rule of thumb is: the older the means of communication, the more protection the law affords it. As Elliot Spitzer said when he was New York State Attorney General, "Never write when you can talk. Never talk when you can nod. And never put anything in an e-mail because it's death. You're giving prosecutors all the evidence we need."

Telephone Communications

Telephone conversations can be intercepted in a variety of ways – from taps to bugs to roving wiretaps to pen registers to trap-and-trace devices. Methods of telephone surveillance are detailed and complex and we can only offer an overview of them here. The lesson, however, is simple – be very careful about what you say on the telephone.

When Can the Government Tap My Phone Calls?

The government generally needs a special warrant called a Title III Wiretap Order to tap your phone. The government can, however, also tap your phone without a warrant for 48 hours under certain emergency situations involving immediate death or serious injury, national security or activities

When Can the Government Tap My Phone Calls? (continued...)

characteristic of organized crime. The government can later seek a warrant to authorize continued surveillance that includes the prior wiretapping.

Title III Wiretap Orders

Title III Wiretap Orders are the warrants that are used to intercept and monitor your communications. In addition to the Fourth Amendment protections requiring search warrants for most searches, Congress provided additional protections regarding oral communication in Title III of the Omnibus Crime Control and Safe Streets Act (1968). These increased protections were passed in response to the Congressional findings of widespread illegal and abusive surveillance by the FBI in the 1960s (See "Are There Limits on What Undercover Agents and Informants Can Do?").

Agents must file a lengthy Title III application that includes: facts regarding the crime that has been or is about to be committed; the place from which communications will be intercepted; the communications sought to be intercepted; whether other investigative tools have been utilized and were inadequate or that other tools would be inadequate or too dangerous to apply; the time frame for interceptions to occur; and a statement on all previous wiretap applications concerning the same target or premises.

To issue a Title III Wiretap Order, a judge must find: probable cause that the target is committing a crime covered under Title III; that communication concerning that crime will be obtained by the interception; and that the facilities from which communication will be intercepted are being used in connection with the crime.

⚠ Know Their Tools

Title III Wiretap Orders (cont.)

Originally, Title III only permitted surveillance for a narrow category of serious crimes. Over the years, Congress has added more and more crimes Title III's coverage. Today, the law covers hundreds of crimes, including broad categories such as crimes involving drugs, riots, obscenity or interference with commerce. Such broad interpretations of these crimes allow for the surveillance of many forms of activism.

Title III Wiretap Orders may initially last for up to 30 days. Law enforcement can return to the judge for repeated 30 day extensions. After a Title III Wiretap Order expires, the judge can order the government to disclose an inventory of intercepted communications to the targets of the wiretap. Such an inventory informs the targets of the time period of the wiretap and whether communications were actually intercepted. The judge may choose, however, to not require that such an inventory be issued.

Generally, it is rare practice for law enforcement to seek wiretap orders; but they almost always get them when they ask. For example, in 2007, only 2,208 applications for wiretap orders were submitted to the state and federal courts, but every single application was granted in that year. The vast majority of the wiretap orders were in narcotics cases (1,792 out of 2,208 or 81 percent), with the next highest being homicide and assault cases (132 out of 2,208 or 6 percent).

Know Their Tools

How Will I Know If My Phone Is Being Tapped?

Most likely, you will not know if your phone is tapped. Government surveillance has made great strides since the time when clicks, beeps, buzzing or any other sound might tip you off to a tap. The government is generally supposed to tell you within 90 days after the surveillance ends, but notification can be postponed with relative ease.

What Is a Roving Wiretap?

Typically, a wiretap is applied to a specific phone at a specific location after it has been authorized through a court order. A roving wiretap, however, is a tap on any phone at any location from which the law enforcement agent believes the target will be making phone calls. Roving wiretaps have been allowed for government use since 1998. The government needs to meet the same standard for a roving wiretap as they do for a regular tap – probable cause that a crime has been or is about to be committed.

What About Bugs?

A bug is a miniature electronic device that can overhear, broadcast and/or record a conversation. By placing a bug in your home or office, law enforcement can listen in on everything that is said within the device's range. The requirements governing the use of bugs are generally the same as those for wiretaps. The use of bugs presents some inherent difficulties for law enforcement agents: they must be installed within the target location; they are prone to malfunction; there is a risk of discovery; and they may be rendered useless by electrical interference. Because of these difficulties, bugs are likely used to a lesser degree than wiretaps.

Pen Registers and "Trap and Trace" Devices

A pen register device records the numbers dialed from a telephone line to which the device is attached. "Trap and trace" devices record the telephone numbers of incoming calls.

A court order is required if law enforcement wants to install and use either device; however, these court orders are very easy to obtain. The government needs only to believe that the information likely to be obtained is relevant to an ongoing criminal investigation. Judges and law enforcement typically take a very broad view of what is likely to be relevant to an investigation. Many states allow such surveillance under even more lax standards. Also, the U.S. Attorney General can in certain

Know Their Tools

Pen Registers and "Trap and Trace" Devices (cont.)

"emergency" situations authorize the use of these devices for up to seven days without seeking an order from the judge.

The Patriot Act expanded the permitted use of both of pen registers and trap-and-trace devices. Some expanded uses of pen registers and trap-and-trace devices include: tracking the physical location of cell phone users; recording the addresses of Web sites you visit; the Internet Protocol (IP) addresses that your computer connects to; or the IP addresses of computers that connect to your computer. An IP address is a unique number assigned to each computer or device that connects to a network.

Know Their Tools

What About the Foreign Intelligence Surveillance Court and the National Security Agency's Warrantless Wiretapping Program?

The government can wiretap both citizens and noncitizens if there is probable cause to believe that the target is a member of a foreign terrorist group or an agent of a foreign power. In order to wiretap citizens and lawful permanent residents, the government must also demonstrate probable cause that the target is engaged in activities that "may" involve a criminal violation. For this type of surveillance, the government must obtain a search warrant from the Foreign Intelligence Surveillance Court, a secret court in which hearings and records are closed to the public. The government, via the National Security Agency (NSA), claims the authority to warrantlessly monitor any telephone or electronic communication if it believes one party is located outside of the U.S. – even if the other party is inside the U.S. While the NSA is only authorized to monitor communications for purposes of obtaining foreign intelligence, the full scope of the program is unknown.

What Security Threats Do Cellular Phones, Smartphone and PDAs Pose?

The convenience and ease of cell phone communication comes with significant privacy and security risks. Be aware of the risks inherent in using these devices and weigh the convenience benefit to the security risk before each cell phone use.

The same legal rules that apply to landlines apply to getting a tap, pen register or trap-and-trace device on a cell phone. It is important to note, however, that anyone with a few hundred dollars worth of equipment can intercept your cell phone signals. And, you shouldn't assume that agents always follow the law. Individuals and corporations may also easily intercept your cell phone signals with little risk of being caught.

The government has the ability to turn a cell phone into a listening device or a "roving bug." This allows the government to hear any conversations that take place near the cell phone. The government does not need access to the cell phone itself to "plant" a roving bug, but can simply initiate it through your cell phone company. Roving bugs allow the government to hear conversations near your cell phone even when it is turned off. It appears, however, that physically removing the battery from a cell phone will disable a roving bug.

Your cell phone can also be used to track your location. Whenever your cell phone is on and has a signal, it is in contact with one of more cellular towers in your area. The government can monitor these connections to determine your physical location. In cities and other areas with a higher density of cellular towers, your location can be tracked more precisely, sometimes within a few yards. Currently, there is no uniform legal standard for this kind of cell phone tracking. Some courts require agents to meet the same low showing needed to obtain a pen register or trap-and-trace device while other courts require agents to obtain a warrant supported by probable cause. The government can also go through your past cell phone records to determine your location at that time if your cell phone was turned on.

Some courts have held that once you are arrested, law enforcement can, with a warrant, search the call history and contacts stored in your cell phone. Some courts have even held that, after a lawful arrest, law enforcement can search text messages, pictures, e-mails and any other records contained on your phone. Some courts allow law enforcement to search call histo-

What Security Threats Do Cellular Phones, Smartphone and PDAs Pose? (continued ...)

ries without a warrant, with the argument that the call history will yield the same information that can obtained by a pen register, but require a warrant for searching text messages or e-mails. The courts are still developing this area of law; as a result, laws and regulations vary from jurisdiction to jurisdiction. Enabling password protection on your cell phone offers some level of protection against the security risks inherent in cell phone usage.

Can the Government Monitor My Text Messages?

Text messaging is a considerably insecure method of communication. Like cell phone conversations, text messages can be easily intercepted by anyone with the right equipment. Neither Congress nor the courts have been clear about whether probable cause and a warrant are required to intercept text messages, so law enforcement may attempt to intercept text messages using pen registers or trap-and-trace orders which are relatively easy to obtain. Finally, because text messages are not considered "wire communications," they are not protected by the exclusionary rule of the Wiretap Act. So even if the government illegally intercepts your text messages, it can still use these communications against you in a criminal trial.

Internet Communications

Can the Government Read My E-mail?

Law enforcement can easily access much of your electronic communications and the information they contain. To obtain a subpoena to access your electronic communications, the government needs only to demonstrate that the information likely to be obtained is relevant to an ongoing criminal investigation. With the subpoena, the government can obtain your "basic subscriber information," which includes the name and physical address associated with an account; the length and types of service used; session logs; and the IP address of your computer.

The government needs a D Order (see "Know Their Tools: D Orders") to obtain other "non-content records," which include any records or logs that reflect the e-mail addresses you send e-mail to or receive e-mail from; times and dates on which e-mails were sent or received; and the size of each e-mail.

Regarding e-mail stored by a third party, such as a Web e-mail service or an Internet Service Provider (ISP), different protections apply depending on how recent an e-mail is and whether or not you have read it. The Stored Communications Act requires law enforcement to obtain a search warrant for the content (subject line and body) of unopened emails that have been in storage for less than 180 days. For unopened e-mails older than 180 days and for opened e-mails in storage by the third party, the government can obtain a D Order or issue a subpoena for the content of the emails. The government can also choose to get a search warrant for emails older than 180 days or opened emails.

In Alaska, Arizona, California, Hawaii, Idaho, Montana, Nevada, Oregon and Washington, which are states covered by the Ninth Circuit Court of Appeals, courts have disagreed with the government's interpretation that it can, with a D Order, obtain opened e-mails that has been in storage for less than 180 days. These courts have ruled that the government needs a warrant for any e-mail that is less than 180 days old.

The government is supposed to give the individual subscriber prior notice before using D Orders or subpoenas to obtain the content of email. In theory this would allow the subscriber to move to quash the subpoena before the third-party complies with it. Another provision of the Stored Communications Act, however, allows law enforcement to delay notice of a D order or subpoena for a substan-

Can the Government Read My Email? (continued ...)

tial period of time, and it appears the government regularly delays notice. Law enforcement can also avoid giving you any notice by taking the extra steps required for a search warrant.

Larger ISPs reportedly receive more than 1,000 subpoenas each month seeking information about their users. Most of the subpoenas request users' names, addresses, ISP addresses and records of when the target signed on and off of the Internet.

There are many reports of law enforcement programs designed to capture vast amounts of Internet traffic, including e-mails and Web activity. The extent of these programs, their permitted use and the admissibility of any information obtained through them in court is currently unknown.

Can the Government Tell What Web Sites I Visit?

Law enforcement needs a warrant for records of the actual Web sites you visit. The government can reportedly obtain the Uniform Resource Locator (URL) addresses, e.g. http://ccrjustice.org, of Web sites you viewed without a warrant; but, the government needs a warrant to obtain information on specific pages you visit on Web site, e.g., http://ccrjustice.org/ifanagentknocks.

"D Orders"

Another law enforcement tool is the 2307(D) Order, commonly referred to as a "D Order." The D Order gets its name from the subsection of the Stored Communications Act that authorizes them. The government uses D Orders to obtain electronic records stored by third parties – most often, email. D Orders are harder to get than a simple subpoena but easier to obtain than a search warrant. To obtain a D Order, the government must provide specific facts to a judge showing there are reasonable grounds to believe the information sought is relevant to an ongoing criminal investigation. So the suspicion required for the D Order is lower than probable cause, but it is higher than the standard of "any reasonable possibility" required in order to obtain a subpoena.

⚠ Know Their Tools

Should I Be Wary of Electronic Surveillance From Non-Governmental Entities?

Corporate spying is likely a larger industry than government spying. Corporations routinely hire private spies, most of whom are former law enforcement agents, to conduct surveillance of activists who may threaten their interests. Corporate spying involves many of the same tactics employed by the government, including: rummaging through trash; tapping telephones; monitoring Internet activity; and using infiltrators. Corporate spies are probably less likely to be concerned by legal restraints on spying.

National Security Letters

The National Security Letter (NSL) is tool used by the FBI to secretly demand information about an individual from a third party, such as a telephone company, ISP, consumer credit agency or financial institution. NSLs require no probable cause or oversight – the FBI only needs to believe the information they seek is relevant to a terrorism or espionage investigation. The NSL law has a built-in gag rule that prohibits someone who receives an NSL from telling anyone except their attorney that they have received one. Though a recent court ruling found the permanent, built-in gag rule unconstitutional, its future application remains unclear.

Government studies have reported that the FBI issues tens of thousands of NSLs a year, and often violates even the minor restraints on their authority to issue these letters. Data from NSLs is shared within the U.S. intelligence community, other government agencies and even foreign governments.

If you or an organization you work with receives a NSL, contact an attorney immediately.

⚠ Know Their Tools

Electronic Security

Electronic security is an immense and complex topic. This section introduces some basic advice regarding electronic security. You will find more in-depth information on each of these topics in the Additional Resources section of this booklet.

Simply put, the most secure electronic communication is no electronic communication at all. Effective electronic security habits require maintaining a constant balance between the convenience and the risks associated with electronic communication. As with any practice, you should weigh risks against rewards when deciding what electronic security measures to employ.

Data Encryption

Encryption is a method of turning information into a ciphered code. If used properly, encryption protects your data from being viewed by anyone who does not have the proper "key" to view it. Modern encryption technology is strong enough so that it is virtually impossible for the government to unscramble encrypted messages without the use of keys. Encryption is the strongest protection you have to prevent the government from obtaining your electronic data.

Widely available programs allow you to encrypt all of the data on your hard drive. Simple passwords to login to your computer are not enough to protect your hard drive. The government can take the hard drive, make a copy of it and easily access the data without your log-in. With an encrypted hard drive, your files will be encoded and the government will not be able to access them without your encryption password.

Encryption programs also allow for encryption of individual files or folders. While this may be easier to manage, piecemeal encryption may allow for additional vulnerabilities to those files. A better solution is to keep a separate, fully encrypted hard drive for sensitive files.

Know Your Tools

Electronic Security

Email Encryption

Using encryption is even more important for e-mail. We've already shown how the government can use D Orders or subpoenas to easily access your e-mails or use other tools to intercept them in transmission. And, once an e-mail is on a third party's computer, you have no control over who can get it and read it. Similar to data encryption, one tool to protect your electronic communications is e-mail encryption. In order to use e-mail encryption effectively, however, both you and whoever you are communicating with must use an encryption program.

E-mail encryption ensures that only the intended recipients can read the e-mail you send. Modern e-mail encryption works through a system of "public keys." A public key provides instructions, or the code, for how e-mails sent to you should be scrambled. The code to unscramble messages – the "private key" – is different from the public key, and only you have access to the private key. If your e-mails are intercepted through a subpoena, court order or otherwise, the messages contained therein cannot be unscrambled without your private key.

While the more technical aspects of e-mail encryption are too detailed to include in this booklet, a simple analogy to encryption is an open door that can be locked by anyone but can be opened only by someone with a special key.

E-mail encryption is easier to use today than it was in the past. GNU Privacy Guard (GnuPG) is a free program that can be integrated into most major e-mail programs. For example, the third party mail client Mozilla Thunderbird offers a plug-in, also known as a security extension, called Enigmail that is compatible with GnuPG and makes encryption fairly easy to use.

Know Your Tools

Electronic Security

Passwords

Take passwords seriously. Don't use a word or a word with a number at the end or in the middle. Those passwords can be easily broken after a few attempts. Use a series of characters that make sense only to you.

Don't use the same password twice for any account that has private information. Try to keep your passwords in your head. Written password can be discovered or subpoenaed. Change your passwords every couple of months. If you do write your passwords down, try to write them in a code only you understand. If you decide to write down a password, never leave it next to or near your computer; you're better off keeping them in your wallet.

Consider using a "password safe" program. These programs allow you to keep your passwords in a single encrypted file on your computer so you only need to memorize one password to access all your other passwords. Do not write your master password down, since it is the password that protects all others.

Web Browsing

Carefully manage the data that your Web browser may keep regarding your Internet activity and the data that other Web sites may have about you.

As a default, Internet browsers keep a great deal of potentially private information, including but not limited to: the Web sites you visit; passwords for those Web site; and even images from the Web pages you visit. An agent who gets a hold of your hard drive can learn a lot about your Internet activity from these files. Delete this information regularly. Set your browser to delete your Internet browsing history, cache, cookies, download history, saved forms and saved passwords regularly. You may want to do this daily or whenever you close your browser.

Whenever available, use a website's built-in encryption when browsing to prevent third parties from intercepting the information transmitted. Web sites that have built-in encryption start with https:// instead of http://. Consider using anonymous Internet tools such as Tor. Tor is

Know Your Tools

Electronic Security

Web Browsing (continued ...)

an encryption and anonymization program that routes your data only through other Tor clients, encrypting your data along the way and stripping out information regarding where the data originated. Each Tor router only knows the address of the last router it went through, making it extremely difficult to trace any communication back to its original source. Some drawbacks to using Tor are slower speeds at which Web pages load, and many unsecured functions such as Flash do not work over Tor.

Know Your Internet Service Providers

Read the terms of service and the privacy policies of any electronic service you are considering signing up for. Some ISPs, including several that are tailored to the needs of political activists, provide stronger privacy protections and claim to be more resistant to government snooping.

Use Anti-Spyware Programs

Purchase a good anti-spyware and/or anti-virus program and regularly update them. Spyware can breach all of your electronic security, logging every Web site you visit and every keystroke on your machine. Major anti-spyware companies claim they treat government spyware the same as any other spyware.

Data Retention and Deletion

The government can't get what doesn't exist. Establish a data retention policy in which you review and delete old files on a consistent basis. Do not selectively destroy documents – pick a time frame and stick to it. You can establish a different schedule for different types of data, e.g., delete computer files every two months; delete emails every two weeks; and delete Web browser logs every two days. Whatever the policy is, stick with it. After all, do you really need the last three years of e-mails?

Do not destroy anything that has

Know Your Tools

Electronic Security

Data Retention and Deletion (continued...)

been subpoenaed – if you do so, you run the serious risk of an obstruction of justice charge. Keep a written record of your data retention policy to protect yourself and your organization against accusations of destroying evidence.

Know Your Tools

Grand Juries & Grand Jury Resistance

What are Grand Juries and What Threats Do They Pose to Activists?

A grand jury is a panel of citizens brought together to investigate crimes and issue indictments. In their original conception, grand juries were intended to be radically democratic. In England, they served as a buffer between citizens and the monarch and her/his prosecutors. In early America, any citizen could bring an allegation of wrongdoing to the original grand jury and the grand jury could indict on a majority vote.

Modern day grand juries are very different. Today, all cases are brought to a grand jury by a prosecutor. The prosecutor picks the witnesses and asks the questions. Witnesses are not allowed to have a lawyer present. There is no judge present. The prosecutor drafts the charges and reads them to the grand jury. There is no requirement that the grand jury members be instructed on the law at issue. And, unlike in other juries, grand jury members are not screened for bias.

Since the prosecutor solely orchestrates the proceedings, it is no surprise that grand juries almost always serve as a rubber stamp for prosecution. A former chief judge of New York once famously noted that "any prosecutor that wanted to could indict a ham sandwich." In the rare event that a grand jury does not indict, the prosecutor can simply impanel a different grand jury and seek an indictment before a new grand jury.

In political cases, grand juries have been used to execute witch hunts against activists. Prosecutors will bring in activist witnesses and attempt to get them to snitch

What are Grand Juries and What Threats Do They Pose to Activists? (continued...)

on other activists with threats of jail time if they refuse to cooperate with the grand jury. It is critical to understand how a grand jury works; what your rights are; what rights you cannot exercise; and how to resist a grand jury.

Many rights we take for granted do not exist for grand jury witnesses. Grand jury witnesses have no right to be represented by an attorney and no right to a jury trial if they are threatened with jail. Grand jury witnesses do retain the right against self-incrimination but can nonetheless be forced to snitch on themselves and others in exchange for immunity from prosecution and punishment. Immunity only protects witnesses – others can still be prosecuted.

What Should I Do If Someone Shows Up With a Grand Jury Subpoena?

Grand jury subpoenas are served by law enforcement agents, usually police officers or federal marshals. A grand jury subpoena must be personally served on you, meaning, it must be handed to you. If you refuse to accept it, it must be placed near you.

A grand jury subpoena does not give an agent the right to search a home, office, car or anywhere else, nor does it require you to relinquish any documents or say anything at that time. A grand jury subpoena is only requires you to do something on the future date stated on the subpoena.

If an agent shows up and tries to serve you with a subpoena, take it and do not do anything else. Do not answer any questions; do not consent to a search; and do not invite them into your home for any reason.

Grand Jury Subpoenas

Grand juries get information from people by issuing subpoenas. A grand jury subpoena is an order to testify before a grand jury or provide the grand jury with certain information. Grand juries issue different types of subpoenas for testimony and information. A subpoena ad testificandum, or testifying, is a subpoena ordering a witness to appear and give testimony. A subpoena duces tecum, which means "bring it with you" in Latin, is a subpoena ordering a witness to provide the grand jury with certain documents. Grand juries also use these orders to obtain fingerprints and handwriting samples. Grand juries often issue both subpoenas to the same witness so they can obtain both documents and testimony.

⚠ Know Their Tools

What Options Do I Have If I Receive a Grand Jury Subpoena?

Once you have received a grand jury subpoena, you typically have three options: 1) You can comply with the subpoena; 2) you can move to quash the subpoena; or 3) you can refuse to comply. If you receive a subpoena, you should contact an attorney as soon as possible and discuss each of these options in detail.

Complying with a subpoena is relatively straightforward. For a *subpoena ad testificandum*, you arrive at the date, time and location stated on the subpoena and answer the prosecutor's questions. For a *subpoena duces tecum*, you show up on the date, time and location stated on the subpoena with the documents or other evidence required.

If you comply with a subpoena, you avoid the possibility of being punished for ignoring it; however, complying with a subpoena may get you into a different type of trouble. For example, if you are a target of the investigation, complying with the subpoena may provide the government with information it might need to charge and convict you. You might also place another activist in jeopardy by complying with a subpoena.

If you receive a subpoena, you should speak with a lawyer before taking any action. If the subpoena is politically motivated, it is best to speak with an attorney in your activist circle who does criminal defense or grand jury work. Some

What Options Do I Have If I Receive a Grand Jury Subpoena? (continued...)

non-activist criminal defense attorneys may suggest you become a snitch. It is important to note, however, that many snitches end up serving as many years in prison as the individuals on whom they snitched.

Grand jury proceedings are secret. The activist community often does not know when a grand jury investigation is being pursued. As a result, many activists believe that they should publicize the fact that they have received a subpoena. This may be an effective tactic to explore with your attorney if you receive a subpoena.

How Do I Quash a Grand Jury Subpoena?

You can challenge a subpoena in court by a motion to quash the subpoena. Quashing a subpoena means a court declares it null and void. A court will only grant a motion to quash if there is a sufficient legal basis, such as misidentification; lack of jurisdiction; a protected privilege; or an unlawful basis of the proceedings.

Even if you cannot successfully quash a subpoena, litigating a motion to quash in court can buy you some time. Time is important, especially if you do not plan to cooperate with the grand jury, because non-cooperation can land you in jail. Grand juries can last for as long as 18 months; whatever time is spent litigating the motion to quash may save you the experience of spending that entire period in jail.

While there is little to lose by filing a motion to quash a *subpoena duces tecum*, the subpoenas that demand evidence, motions to quash *subpoenas ad testificandum*, which demand testimony, can present problems. At least one federal circuit court ruled that you lose any objections that was not raised in the original motion to quash. You should not waive your objections, especially because you may not know what your objections are until you are asked a particular question.

A good political attorney should be able to provide advice on whether moving to quash a subpoena is a good idea or not in your particular circumstances.

What Happens If I Refuse to Comply With a Grand Jury Subpoena?

There are two basic ways to refuse to comply with a grand jury subpoena: 1) refuse to show up; and 2) refuse to answer any of the prosecutor's questions.

If you simply refuse to show up for your testimony, you may be in contempt and the government can choose to arrest you and jail you until you testify or until the grand jury expires. If your testimony is not particularly important to the prosecutor, they may choose not to take action.

What Happens If I Comply With a Grand Jury Subpoena?

If you appear to testify, you will not be allowed to have an attorney present. You can, however, have an attorney just outside the grand jury room, and you can consult with her/him after every question, although some courts have ruled you can only consult your attorney after every few questions.

Because you retain your Fifth Amendment right against self-incrimination, you can refuse to answer the prosecutor's questions by saying "I invoke my Fifth Amendment privilege against self-incrimination" after every question. At this point, the prosecutor may simply dismiss you or s/he may seek to grant you immunity.

Immunity prevents the witness from having criminal charges brought on the basis of the grand jury testimony. A judge must approve a grant of immunity. A prosecutor can get a judge to pre-approve a grant of immunity; otherwise, a witness is brought before a judge who, upon the prosecutor's request, virtually always grants immunity.

If you continue to refuse to answer questions after being granted immunity, the prosecutor can bring you before a judge, and the judge will order you to testify. If you continue to refuse, the judge can have you jailed for civil contempt. Witnesses who refuse to provide physical exemplars, i.e. samples of handwriting, hair, appearance in a lineup or documents, upon the request of a grand jury may also be jailed for civil contempt.

While civil contempt is not a crime, it can result in the witness being jailed for the duration of the grand jury. Grand juries can last for up to 18 months, although some "special" grand juries can obtain up to three extensions of six month periods each. The purpose of incarcerating a recalcitrant witness is to coerce her/him to

What Happens If I Comply With a Grand Jury Subpoena? (continued...)

testify. Judges will sometimes free witnesses before the expiration of the jury if it is clear that there is no chance the witness will testify.

The government can also use the charge of "criminal contempt" against uncooperative grand jury witnesses. Criminal contempt carries no maximum penalty – the sentence depends entirely on the judge's discretion. While civil contempt is meant to coerce a witness to testify, criminal contempt is meant to punish a witness for impeding the legal process. As with any other crime, criminal contempt requires notice of the charges, the right to receive assistance of counsel, and proof beyond a reasonable doubt. Charges of criminal contempt are extremely rare.

If you are jailed, you can periodically file a motion stating that: 1) jail will not coerce you into testifying; and 2) your confinement is merely punitive and therefore unconstitutional. If you win one of these motions, you will be released.

Some activists create files to prepare for being called before a grand jury. A file that memorializes your stalwart belief against cooperating with grand jury proceedings can be used as evidence that civil contempt will not work to coerce you and thereby help you win release.

What Happens After a Grand Jury?

What takes place in grand jury proceedings is secret. The government relies on this secrecy to create fear and distrust in activist communities. Some activists have successfully dispelled that fear and distrust in activist comities by publishing the questions asked of them by the prosecutor and the answers they provided. If you are considering taking action in this way, you must talk with an attorney to ensure that you are not creating more problems than you are solving.

Special Considerations for Noncitizens

Noncitizens are individuals who do not have U.S. citizenship, including tourists, students and others who are in the U.S. on visas or visa waiver programs; lawful permanent residents; refugees; and those without legal immigration status. Noncitizens in the U.S. share most of the same constitutional rights as citizens. There are some exceptions to that rule, and noncitizens engaging in political activism should be aware of several special considerations. Noncitizens should not, however, entirely avoid political activism based on an unreasonable fear of government repression.

Speech and Political Affiliations

In most cases, the government treats speech by noncitizens in the same way it treats speech by citizens. Noncitizens cannot be criminally punished for speech that would be protected if uttered by a citizen. Similarly, noncitizens cannot be sued for speech that would be protected if said by a citizen.

The government does, however, have broad powers to withhold immigration benefits (such as discretionary relief or naturalization) and may potentially even initiate removal proceedings based on a noncitizen's speech. It is unclear whether the government can remove a noncitizen or withhold discretionary benefits for speech or political association alone. Fifty years ago, some courts found the government could, but First Amendment law has changed dramatically since then, and courts are now split on whether that rule is still good law. Practically speaking, it is extremely rare for the government to remove someone based purely on speech or association. The government, however, is allowed to selectively enforce immigration laws. For instance, the government can remove nonciti-

Speech and Political Affiliations (continued...)

zens for violations of immigration law (such as overstaying a visa or working without authorization) even if the government's motivation in initiating removal proceedings is a noncitizen's speech or political association.

Finally, applicants for permanent residence and naturalization are asked to list the organizations with which they have worked. Politically active noncitizens are advised to consult an immigration lawyer before applying for a change in status because some associations may cause problems in your application process.

Searches and Seizures

Noncitizens largely enjoy the same Fourth Amendment protections against unreasonable searches and seizures that citizens do. Law enforcement must get a warrant to perform any search on a noncitizen or a noncitizen's property just as they must to perform a search on a citizen. Evidence obtained in violation of the Fourth Amendment is excluded from a noncitizen's criminal trial the same way it is for citizens.

Unfortunately, the use of evidence obtained in violation of the Fourth Amendment is generally permissible in immigration proceedings. This means the government can use illegally obtained evidence that cannot be used in criminal proceedings for immigration proceedings. It is possible that evidence obtained through especially egregious violations of the Fourth Amendment may be excluded in immigration proceedings.

Also, the government can generally search and seize any person, package or vehicle traveling across the border or at an airport.

Right to Remain Silent

Noncitizens generally have the same right to remain silent that citizens do. If questioned by law enforcement agents, you can remain silent and refuse to answer their questions even if they detain you temporarily or arrest you. You can simply say nothing or say something like "I'd like to talk to my lawyer before I say anything to you," or "I have nothing to say to you. I will talk to my lawyer and have her/him contact you." Do not sign anything without reading and fully understanding the consequences of signing it.
One exception to this rule is if an immigration officer asks a noncitizen to provide information related to her/his immigration status; however, even in this situation, you can still state that you would like a lawyer present before you answer any questions.

Right to Remain Silent (continued...)

The law also requires adult noncitizens with have valid immigration documents to carry these documents at all times. If an agent asks for your documents and you refuse to provide them, you can be charged with a misdemeanor.

Never show fake immigration papers or claim that you are a U.S. citizen if you are not. Instead, you should remain silent or say you would like to talk to a lawyer. Lying to a federal agent is a much more serious crime than the misdemeanor of failing to produce documents – it is better not to produce anything than to produce false documents. Also, falsely claiming to be a citizen may bar you from obtaining lawful status or citizenship in the future.

Conclusion

As noted before, the information presented in this booklet is a primer on your basic rights. This guide is meant to help you prepare yourself, your organization and your fellow activists to be fully informed and protected in the event that an agent knocks at your door. And remember, different states have different laws – it is a good idea to learn the laws of your state and to have access to a lawyer who is familiar with them.

We hope this booklet can be a tool for you and your organization as we work towards a more socially just world.

For copies of this publication, visit http://ccrjustice.org/ifanagentknocks or write directly to iaak@ccrjustice.org.

Additional Resources

About General Security Practices

Security Culture: a Handbook for Activists: An excellent zine by Canadian activists on why to build a security culture and how to do it.
http://security.resist.ca/personal/culture.shtml

Security Survival Skills, by the Collective Opposed to Police Brutality: An explanation of how to build security culture in your activist community from a group in Canada.
http://www.why-war.com/files/Securite-eng-letter.pdf

War at Home, by Brian Glick: An extensive book on the history of COINTELPRO and excellent advice on how to avoid the same pitfalls and protect yourself and your community. Published by South End Press.

About Government Agents

The Attorney General's Guidelines on FBI Undercover Operations: the Federal Government's rules on what undercover agents can and cannot do.
http://www.usdoj.gov/olp/fbiundercover.pdf

The Attorney General's Guidelines Regarding the Use of Confidential Informants: The Federal Government's rules on what informants can and cannot do.
http://www.usdoj.gov/olp/dojguidelines.pdf

Security Practices and Security Culture: basic tips on dealing with covert operations and great anecdotes from the COINTELPRO era.
http://aia.mahost.org/sec_cointelpro.htm

About Telephone Security

Mobile Surveillance Primer: a thorough online resource on cell phone technologies, how they can be accessed, and how to protect the information stored on them and your conversations.
http://mobileactive.org/wiki/Mobile_Surveillance-A_Primer

About National Security Letters

A Review of the FBI's Use of National Security Letters, by the Department of Justice: an in-depth review of the law on National Security Letters and how they've been used since their inception.
http://www.usdoj.gov/oig/special/s0703b/final.pdf

About Computer Security

Computer Security Trainer's Guide, by Midnight Special Law Collective: A really excellent guide to developing good security habits with computers rather than software or technical tricks.
http://www.midnightspecial.net/materials/trainers.html

NGO in a Box: Security Edition, by Tactical Technology Collective and Front Line Human Rights Defenders: A toolkit to help activists and independent media makers establish digital security and protect their privacy. The toolkit includes guides on encryption tools; virus, adware and spyware cleaner tools; data storage; password protection; etc. Available for free on the internet.
http://security.ngoinabox.org

Surveillance Self Defense, by Electronic Frontier Foundation: an excellent online resource on how to protect yourself from all types of electronic surveillance. For specifics on computer security, check out "Data Stored on Your Computer" and "Defensive Technology."
https://ssd.eff.org

About Hi-Tech Surveillance

Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society, by the ACLU: a white paper about the recent history of surveillance cameras and other technologies.
http://www.aclu.org/FilesPDFs/aclu_report_bigger_monster_weaker_chains.pdf

About Grand Juries

Grand Jury Trainers Guide, by Midnight Special Law Collective: an explanation of grand juries – from first contact with federal agents to the Grand Jury hearing itself – and how to protect yourself and your community if you are called before one.
http://www.midnightspecial.net/materials/trainers.html#gj

Disclaimer: This booklet is for informational purposes only and does not constitute legal advice. CCR aims to provide a general description of the legal and practical issues that progressive or radical activists might face. Each person's circumstances are unique, and minor factual differences may result in very different answers to the questions presented here. For answers to specific legal problems, issues or questions, obtain the advice of a qualified attorney in your area.

Acknowledgements & Credits

Third Edition published September 2009

Center for Constitutional Rights
666 Broadway, 7th Floor
New York, NY 10012
www.CCRJustice.org / (212) 614-6464

The Center for Constitutional Rights (CCR) is dedicated to advancing and protecting the rights guaranteed by the United States Constitution and the Universal Declaration of Human Rights. Founded in 1966 by attorneys who represented civil rights movements in the South, CCR is a non-profit legal and educational organization committed to the creative use of law as a positive force for social change. Visit www.ccrjustice.org.

Principal author, Matthew Strugar, CCR Staff Attorney.
"If an Agent Knocks" was prepared by CCR staff and interns, including Lauren Melodia, Rachel Meeropol, Alison Roh Park, Qa'id Jacobs, Jeff Deutch, Arwa Fidahusein, Cathe Giffuni, Toni Holness, Carolyn Hsu, Jessica Juarez, Kenneth Kreuscher, David Mandel-Anthony and Christina Stephenson.

Cover artwork by Robert Trujillo (2009)
Photography by Maddy Miller (pp. 5,9,15)
Photography by SSGT Reynoldo Ramon, USAF (p. 21)
Photography by Jarek Tuszynski (p. 36)
Fonts used: Georgia (body), Distro (headers), Fluoxetine (headers)
Icons by pixel-mixer.com
Layout: Qa'id Jacobs

centerforconstitutionalrights

on the front lines for social justice