What Can I Do To Protect Myself?

In the last section, you learned that wiretapping and pen-trap tapping are powerful and routine government surveillance techniques, and got an idea of how often those techniques are legally used. In this section, you'll learn how to defend yourself against such real-time communications surveillance. As we'll describe in detail below, unless you take specific technical measures to protect your communications against wiretapping or traffic analysis — such as using encryption to scramble your messages — your best defense is to use the communications methods that possess the strongest and clearest legal protections: postal mail and landline telephones.

Threats

What You Are Protecting Against

A *threat* is something bad that can happen to an asset. Security professionals divide the various ways threats can hurt your data assets into six sub-areas that must be balanced against each other:

- **Confidentiality** is keeping assets or knowledge about assets away from unauthorized parties.
- **Integrity** is keeping assets undamaged and unaltered.
- **Availability** is the assurance that assets are available to parties authorized to use them.
- **Consistency** is when assets behave and work as expected, all the time.
- **Control** is the regulation of access to assets.
- **Audit** is the ability to verify that assets are secure.

Threats can be classified based on which types of security they threaten. For example, someone trying to read your email (the asset) without permission threatens its confidentiality and your control over it. If, on the other hand, an adversary wants to destroy your email or prevent you from getting it, the adversary is threatening the email's integrity and availability. Using encryption, as described later in this guide, you can protect against several of these threats. Encryption not only protects the confidentiality of your email by scrambling it into a form that only you or your intended recipient can descramble, but also allows you to audit the emails — that is, check and see that the person claiming to be the sender is actually that person, or confirm that the email wasn't changed between the sender and you to ensure that you've maintained the email's integrity and your control over it.

Assets

What You Are Protecting

An *asset* is something you value and want to protect. Anything of value can be an asset, but in the context of this discussion most of the assets in question are information. Examples are you or your organization's emails, instant messages, data files and web site, as well as the computers holding all of that information.

Adversaries

Who Poses a Threat?

A critical part of assessing risk and deciding on security solutions is knowing who or what your *adversary* is. An adversary, in security-speak, is any person or entity that poses a threat against an asset. Different adversaries pose different threats to different assets with different risks; different adversaries will demand different solutions.

For example, if you want to protect your house from a random burglar, your lock just needs to be better than your neighbors', or your porch better lit, so that the burglar will choose the other house. If your adversary is the government, though, money spent on a better lock than your neighbors' would be wasted — if the government is investigating you and wants to search your house, it won't matter how well your security compares to your neighbors. You would instead be better off spending your time and money on other security measures, like encrypting your valuable information so that if it's seized, the government can't read it.

Here are some examples of the kinds of adversaries that may pose a threat to your digital privacy and security:

- U.S. government agents that follow laws which limit their activities
- U.S. government agents that are willing and able to operate without legal restrictions
- Foreign governments
- Civil litigants who have filed or intend to file a lawsuit against you
- Companies that store or otherwise have access to your data
- Individual employees who work for those companies
- Hackers or organized criminals who randomly break into your computer, or the computers of companies that store your data

- Hackers or organized criminals that specifically target your computer or the computers of the companies that store your data
- Stalkers, private investigators or other private parties who want to eavesdrop on your communications or obtain access to your machines

This guide focuses on defending against threats from the first adversary — government agents that follow the law — but the information herein should also provide some help in defending against the others.

Putting it All Together

Which Threats from Which Adversaries Pose the Highest Risk to Your Assets?

Putting these concepts together, you need to evaluate which threats to your assets from which adversaries pose the most risk, and then decide how to manage the risk. Intelligently trading off risks and costs is the essence of security. How much is it worth to you to manage the risk? For example, you may recognize that government adversaries pose a threat to your webmail account, because of their ability to secretly subpoena its contents. If you consider that threat from that adversary to be a high risk, you may choose not to store your email messages with the webmail company, and instead store it on your own computer. If you consider it a low risk, you may decide to leave your email with the webmail company — trading security for the convenience of being able to access your email from any internet-connected computer. Or, if you think it's an intermediate risk, you may leave your email with the webmail company but tolerate the inconvenience of using encryption to protect the confidentiality of your most sensitive emails. In the end, it's up to you to decide which trade-offs you are willing to make to help secure your assets.

A Few Parting Lessons

Now that we've covered the critical concepts, here are a few more basic lessons in security-think that you should consider before reading the rest of this guide:

Knowledge is Power. Good security decisions can't be made without good information. Your security tradeoffs are only as good as the information you have about the value of your assets, the severity of the threats from different adversaries to those assets, and the risk of those attacks actually happening. We're going to try to give you the knowledge you need to identify the threats to your computer and communications security that are posed by the government, and judge the risk against possible security measures.

The Weakest Link. Think about assets as components of the system in which they are used. The security of the asset depends on the strength of all the components in the system. The old adage that "a chain is only as strong as its weakest link" applies to security, too: The system as a whole is only as strong as the weakest component. For example, the best door lock is of no use if you have cheap window latches. Encrypting your email so it won't get intercepted in transit won't protect the confidentiality of that email if you store an unencrypted copy on your laptop and your laptop is stolen.

Simpler is Safer and Easier. It is generally most cost-effective and most important to protect the weakest component of the system in which an asset is used. Since the weak components are much easier to identify and understand in simple systems, you should strive to reduce the number and complexity of components in your information systems. A small number of components will also serve to reduce the number of interactions between components, which is another source of complexity, cost, and risk.

More Expensive Doesn't Mean More Secure. Don't assume that the most expensive security solution is the best, especially if it takes away resources needed elsewhere. Low-cost measures like shredding trash before leaving it on the curb can give you lots of bang for your security buck.

There is No Perfect Security — It's Always a Trade-Off. Set security policies that are reasonable for your organization, for the risks you face, and for the implementation steps your group can and will take. A perfect security policy on paper won't work if it's too difficult to follow day-to-day.

What's Secure Today May Not Be Secure Tomorrow. It is also crucially important to continually re-evaluate the security of your assets. Just because they were secure last year or last week doesn't mean they're still secure!

Search, Seizure and Subpoenas

In this section, you'll learn about how the law protects — or doesn't protect — the data that you store on your own computer, and under what circumstances law enforcement agents can search or seize your computer or use a subpoena to demand that you turn over your data. You'll also learn how to protect yourself in case the government *does* attempt to search, seize, or subpoena your data, with a focus on learning how to minimize the data that you store and use encryption to protect what you do store.

What Can the Government Do?

Before you can think about security against the government, you need to know law enforcment's capabilities and limitations. The government has extraordinary abilities — it's the best-funded adversary you'll ever face. But the government does have limits. It must decide whether it is cost-effective to deploy its resources against you. Further, law enforcement officers have to follow the law, and most often will try to do so, even if only because there are penalties associated with violating it. The first and most important law for our purposes is the Fourth Amendment to the United States Constitution.

The Fourth Amendment

Protecting People From Unreasonable Government Searches and Seizures

The Fourth Amendment says, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

A *seizure* occurs when the government takes possession of items or detains people.

A *search* is any intrusion by the government into something in which one has a reasonable expectation of privacy.

Some examples of searches include: reaching into your pockets or searching through your purse; entering into your house, apartment, office, hotel room, or mobile home; and examining the contents of your backpack or luggage. Depending on the facts, eavesdropping on your conversations or wiretapping of your communications can also constitute a search and seizure under the Fourth Amendment.

The Fourth Amendment requires searches and seizures to be "reasonable", which generally means that police must get a search warrant if they want to conduct a legal search or seizure, although there are exceptions to this general rule. If a search or seizure is "unreasonable" and thus illegal, then police cannot use the evidence obtained through that search or seizure in a criminal trial. This is called the *exclusionary rule* and it is the primary incentive against government agents violating your Fourth Amendment rights.

A few important things to remember:

- The Fourth Amendment protects you from unreasonable searches whether or not you are a citizen. In particular, the exclusionary rule applies to all criminal defendants, including non-citizens. However, the exclusionary rule does not apply in immigration hearings, meaning that the government may introduce evidence from an illegal search or seizure in those proceedings.

- The Fourth Amendment applies whenever the government — whether local, state or federal — conducts a search or seizure. It protects you from an unreasonable search or seizure by any government official or agent, not just the police.

- The Fourth Amendment does not protect you from privacy invasions by people other than the government, even if they later hand over what they found to the government — unless the government directed them to search your things in the first place.

- Your Fourth Amendment rights against unreasonable searches and seizures cannot be suspended — even during a state of emergency or wartime — and they have not been suspended by the USA PATRIOT Act or any other post-9/11 legislation.

- If you are ever searched or served with any kind of government order, contact a lawyer immediately to discuss your rights. Contact a lawyer any time you are searched, threatened with a search, or served with any kind of legal papers from the government or anyone else. If you do not have a lawyer, pro bono legal organizations such as EFF are available to help you or assist in finding other lawyers who will.

Reasonable Expectation of Privacy

The Fourth Amendment only protects you against searches that violate your *reasonable expectation of privacy*. A reasonable expectation of privacy exists if 1) you actually expect privacy, and 2) your expectation is one that society as a whole would think is legitimate.

This rule comes from a decision by the United States Supreme Court in 1967, Katz v. United States, holding that when a person enters a telephone booth, shuts the door, and makes a call, the government can not record what that person says on the phone without a warrant. Even though the recording device was stuck to the outside of the phone booth glass and did not physically invade Katz's private space, the Supreme Court decided that when Katz shut the phone booth's door, he justifiably expected that no one would hear his conversation, and that it was this expectation — rather than the inside of the phone booth itself — that was protected from government intrusion by the Fourth Amendment. This idea is generally phrased as "the Fourth Amendment protects people, not places."

A big question in determining whether your expectation of privacy is "reasonable" and protected by the Fourth Amendment arises when you have "knowingly exposed" something to another person or to the public at large. Although Katz did have a reasonable expectation of privacy in the sound of his conversation, would he have had a reasonable expectation of privacy in his appearance or actions while inside the glass phone booth? Probably not.

Thus, some Supreme Court cases have held that you have no reasonable expectation of privacy in information you have "knowingly exposed" to a third party — for example, bank records or records of telephone numbers you have dialed — even if you intended for that third party to keep the information secret. In other words, by engaging in transactions with your bank or communicating phone numbers to your phone company for the purpose of connecting a call, you've "assumed the risk" that they will share that information with the government.

You may "knowingly expose" a lot more than you really know or intend. Most information a third party collects — such as your insurance records, credit records, bank records, travel records, library records, phone records and even the records your grocery store keeps when you use your "loyalty" card to get discounts — was given freely to them by you, and is probably not protected by the Fourth Amendment under current law. There may be privacy statutes that protect against the sharing of information about you — some communications records receive special legal protection, for example — but there is likely no constitutional protection, and it is often very easy for the government to get a hold of these third party records without your ever being notified.

Here are some more details on how the Fourth Amendment will — or won't — protect you in certain circumstances:

Residences. Everyone has a reasonable expectation of privacy in their home. This is not just a house as it says in the Fourth Amendment, but anywhere you live, be it an apartment, a hotel or motel room, or a mobile home.

However, even things in your home might be knowingly exposed to the public and lose their Fourth Amendment protection. For example, you have no reasonable expectation of privacy in conversations or other sounds inside your home that a person outside could hear, or odors that a passerby could smell (although the Supreme Court has held that more invasive technological means of obtaining information about the inside of your home, like thermal imaging technology to detect heat sources, is a Fourth Amendment search requiring a warrant). Similarly, if you open your house to the public for a party, a political meeting, or some other public event, police officers could walk in posing as guests and look at or listen to whatever any of the other guests could, without having to get a warrant.

Business premises. You have a reasonable expectation of privacy in your office, so long as it's not open to the public. But if there is a part of your office where the public is allowed, like a

reception area in the front, and if a police officer enters that part of the office as any other member of the public is allowed to, it is not a search for the officer to look at objects in plain view or listen to conversations there. That's because you've knowingly exposed that part of your office to the public. However, if the officer does not stay in that portion of the premises that is open to the public — if he starts opening file cabinets or tries to go to private offices in the back without an invitation — then his conduct becomes a search requiring a search warrant.

Trash. The things you leave outside your home at the edge of your property are unprotected by the Fourth Amendment. For example, once you carry your trash out of your house or office and put it on the curb or in the dumpster for collection, you have given up any expectation of privacy in the contents of that trash. You should always keep this in mind when you are disposing of sensitive documents or anything else that you want to keep private. You may want to shred all paper documents and destroy all electronic media. You could also try to put the trash out (or unlock your trashcan) right before it's picked up, rather than leaving it out overnight without a lock.

Public places. It may sound obvious, but you have little to no privacy when you are in public. When you are in a public place — whether walking down the sidewalk, shopping in a store, sitting in a restaurant or in the park — your actions, movements, and conversations are knowingly exposed to the public. That means the police can follow you around in public and observe your activities, see what you are carrying or to whom you are talking, sit next to you or behind you and listen to your conversations — all without a warrant. You cannot necessarily expect Fourth Amendment protection when you're in a public place, even if you think you are alone. Fourth Amendment challenges have been unsuccessfully brought against police officers using monitoring beepers to track a suspect's location in a public place, but it is unclear how those cases might apply to more pervasive remote monitoring, like using GPS or other cell phone location information to track a suspect's physical location.

Infiltrators and undercover agents. Public meetings of community and political organizations, just like any other public places, are not private. If the government considers you a potential criminal or terrorist threat, or even if they just have an unfounded suspicion that your organization might be up to something, undercover police or police informants could come to your public meetings and attempt to infiltrate your organization. They may even wear hidden microphones and record every word that's said. Investigators can lie about their identities and never admit that they're cops — even if asked directly. By infiltrating your organization, the police can identify any of your supporters, learn about your plans and tactics,

and could even get involved in the politics of the group and influence organizational decisions. You may want to save the open-to-the-public meetings for public education and other non-sensitive matters and only discuss sensitive matters in meetings limited to the most trusted, long-time staff and constituents.

Importantly, the threat of infiltrators exists in the virtual world as well as the physical world: for example, a police officer may pose as a online "friend" in order to access your private social network profile.

Records stored by others. As the Supreme Court has stated, "The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." This means that you will often have no Fourth Amendment protection in the records that others keep about you, because most information that a third party will have about you was either given freely to them by you, thus knowingly exposed, or was collected from other, public sources. It doesn't necessarily matter if you thought you were handing over the information in confidence, or if you thought the information was only going to be used for a particular purpose.

Therefore it is important to pay close attention to the kinds of information about you and your organization's activities that you reveal to third parties, and work to reduce the amount of private information you leave behind when you go about your daily business.

Opaque containers and packages. Even when you are in public, you have a reasonable expectation of privacy in the contents of any opaque (not see-through) clothes or containers. So, unless the police have a warrant or qualify for one of the warrantless search exceptions discussed below, they can't go digging in your pockets or rummaging through your bags.

Laptops, pagers, cell phones and other electronic devices are also protected. Courts have generally treated electronic devices that hold data as if they were opaque containers.

However, always keep in mind that whatever you expose to the public isn't protected. So, if you're in a coffee shop using your laptop and an FBI agent sitting at the next table sees what you are writing in an email, or if you open your backpack and the FBI agent can see what's inside, the Fourth Amendment won't protect you.

Postal mail. The mail that you send through the U.S. Postal Service is protected by the Fourth Amendment, and police have to get a warrant to open it in most cases.

If you're using the U.S. Postal Service, send your package using First Class mail or above. Postal inspectors don't need a search warrant to open discount (media) rate mail because it isn't supposed to be used for personal correspondence.

Keep in mind that although you have privacy in the contents of your mail and packages, you don't have any privacy in the "to" and "from" addresses printed on them. That means the police can ask the post office to report the name and address of every person you send mail to or receive mail from — this is called a "mail cover" — without getting a warrant. Mail covers are a low-tech form of "traffic analysis," which we'll discuss in the section dealing with electronic surveillance.

You don't have any privacy in what you write on a postcard, either. By not putting your correspondence in an envelope, you've knowingly exposed it, and the government can read it without a warrant.

Police at the door: Police in your home or office when it's open to the public?

The police may be able to come into your home or office if you have opened those places to the public — but you can also ask them to leave, just as if they were any other members of the public. If they don't have a warrant, or don't qualify for any of the warrant exceptions, they have no more right to stay once you've asked them to leave than any other trespasser. However, undercover agents or officers need not announce their true identities, so asking all cops to leave the room before a meeting is not going provide any protection.

Search Warrants

Search Warrants Are Generally Required For Most Searches and Seizures

The Fourth Amendment requires that any search or seizure be reasonable. The general rule is that warrantless searches or seizures are automatically unreasonable, though there are many exceptions.

To get a warrant, investigators must go to a neutral and detached magistrate and swear to facts demonstrating that they have *probable cause* to conduct the search or seizure. There is probable cause to search when a truthful affidavit establishes that evidence of a crime will be probably be found in the particular place to be searched. Police suspicions or hunches aren't

enough — probable cause must be based on actual facts that would lead a reasonable person to believe that the police will find evidence of a crime.

In addition to satisfying the Fourth Amendment's probable cause requirement, search warrants must satisfy the particularity requirement. This means that in order to get a search warrant, the police have to give the judge details about where they are going to search and what kind of evidence they are searching for. If the judge issues the search warrant, it will only authorize the police to search those particular places for those particular things.

Police at the door: Search warrants

What should you do if a police officer comes to your home or office with a search warrant?

Be polite. Do not get in the officers' way, do not get into an argument with them or complain, even if you think your rights are being violated. Never insult a police officer. But you should say "I do not consent to this search." If they are properly authorized, they will search anyway. But if they are not, then you have reserved your right to challenge the search later.

Ask to see the warrant. You have a right to examine the warrant. The warrant must tell in detail the places to be searched and the people or things to be seized, and may limit what time of day the police can search. A valid warrant must have a recent date (usually not more than a couple of weeks), the correct address, and a judge's or magistrate's signature. If the warrant appears incomplete, indicates a different address, or otherwise seems mistaken, politely point this out to the police.

Clearly state that you do not consent to the search. The police don't need your consent if they have a warrant, but clearly saying "I do not consent to this search" will limit them to search only where the warrant authorizes. If possible, have witnesses around when you say it.

Do not resist, even if you think the search is illegal, or else you may be arrested. Keep your hands where the police can see them, and never touch a police officer. Do not try to leave if the police tell you to stay — a valid warrant gives them the right to detain any people that are on the premises while the search is conducted. You are allowed to observe and take notes of what the officers do, though they may tell you to sit in one place while they are conducting the search.

Don't answer any questions. The Fifth Amendment guarantees your right not to answer questions from the police, even if they have a warrant. Remember that anything you say

might be used against you later. If they ask you anything other than your name and address, you should tell them "I choose to remain silent, and will not answer any questions without a lawyer." If you say this, they are legally required to stop asking you questions until you have a lawyer with you.

Take notes. Write down the police officers' names and badge numbers, as well as the names and contact information of any witnesses. Write down, as best you can remember, everything that the police say and everything you say to them. Ask if you can watch the search, and if they say yes, write down everything that you see them search and/or seize (you may also try to tape or take pictures, but realize that this may escalate the situation). If it appears they are going beyond what is authorized by the warrant, politely point this out.

Ask for an inventory. At the conclusion of the search, the police should typically provide an inventory of what has been seized; if not, request a copy but do not sign any statement that the inventory is accurate or complete.

Call a lawyer as soon as possible. If you don't have a lawyer, you can call EFF and we'll try to find you one.

Police at the door: Computer searches and seizures

If the police believe a computer is itself evidence of a crime — for example, if it is stolen or was used to commit a crime — they will usually seize it and then search its contents later. However, if the evidence is just stored on the computer — for example, you have computer records that contain information about the person they are investigating — instead of seizing the whole machine, the police may choose to:

- Search the computer and print out a hard copy of the particular files they are looking for (this is rarely done)
- Search the computer and make an electronic copy of the particular files
- Create a duplicate electronic copy of all of the computer's contents (this is called "imaging" or creating a "bitstream copy" of the computer hard drive) and then search for the particular files later

"Sneak and Peek" Search Warrants

"Sneak and Peek" Search Warrants Are Easier to Obtain Than They Used to Be

Generally, police officers serving a warrant must "knock and announce" — that is, give you notice that they are the police and are serving a warrant (although they might not do this if they reasonably suspect that they will be put in danger, or that evidence will be destroyed, if

they give such notice). If they have a warrant, they can enter and search even if you aren't home — but they still have to leave a copy of the warrant and an inventory of what they seized, so you'll know that your place was searched.

However, thanks to the USA PATRIOT Act, it is much easier for law enforcement to get permission from the court to delay notice rather than immediately inform the person whose premises are searched, if agents claim that giving notice would disrupt the investigation. Since the goal is not to tip the suspect off, these orders usually don't authorize the government to actually seize any property — but that won't stop them from poking around your computers.

The delay of notice in criminal cases can last months. The average delay is 30 to 90 days. In the case of super-secret foreign intelligence surveillance to be discussed later, the delay lasts forever — no one is ever notified, unless and until evidence from the search is introduced in open court.

The risk of being targeted with such a "sneak-and-peek" warrant is very low, although rising quickly. Law enforcement made 47 sneak-and-peek searches nationwide from September 2001 to April 2003 and an additional 108 through January 2005, averaging about fifty per year, mostly in drug cases. We don't know how many foreign intelligence searches there are per year — it's secret, of course — but we'd guess that it's much more common than secret searches by regular law enforcement.

Privacy tip: Sneak and peek searches, key-loggers and government spyware

Secret searches can be used to install eavesdropping and wiretapping devices. Secret searches may also be used to install a key-logging device on your computer. A key-logger records all of the keystrokes that you make on the computer's keyboard, for later retrieval by the police who installed it. So if you are concerned about government surveillance, you should check your office computers for new added hardware that you don't recognize — especially anything installed between the keyboard and the computer — and remove it. A hardware key-logger often looks like a little dongle in between the keyboard plug and computer itself. Keyghost is an example of a hardware key-logger.

However, the government also has the capability to remotely install software key-loggers on your computer — or search the contents of your hard drive, or install surveillance capability on your computer — using its own spyware. There were rumors of such capability a few years ago in news reports about a government software program code-named "Magic Lantern" that could

be secretly installed and monitored over the Internet, without the police ever having to enter your house or office. More recently, news reports revealed that the government had in one case been able to hack into a computer remotely and install software code-named "CIPAV" (the "Computer and Internet Protocol Address Verifier"), which gave the government the IP addresses with which the infected computer communicated.

In response to a survey, all of the major anti-spyware companies claimed that their products would treat government spyware like any other spyware programs, so you should definitely use some anti-spyware product to monitor your computer for such programs. It's possible that a spyware company may receive a court order requiring it not to alert you to the presence of government spyware (several of the companies that were surveyed declined to say whether they had received such orders), but you should still use anti-spyware software if only to protect yourself against garden-variety spyware deployed by identity thieves and commercial data harvesters.

Warrantless Searches

There Are Many Fourth Amendment Exceptions to the General Rule of Warrants

In some cases, a search can be reasonable — and thus allowed under the Fourth Amendment — even if the police don't have a warrant. There are several key exceptions to the warrant requirement that you should be aware of.

Consent. The police can conduct a warrantless search if you voluntarily consent to the search — that is, if you say it's OK. In fact, any person who the police reasonably think has a right to use or occupy the property, like a roommate or guest in your home, or a coworker at your office, can consent to the search. You can make clear to the people you share a home or office with that they do not have your permission to consent to a search and that if police ask, they should say no.

Privacy tip: Don't accidentally consent!

If the police show up at your door without a warrant, step outside then close and lock the door behind you — if you don't, they might just walk in, and later argue that you implied an invitation by leaving the door open. If they ask to come in, tell them "I do not consent to a search." Tell roommates, guests, coworkers and renters that they cannot consent on your behalf.

Administrative searches. In some cases, the government can conduct administrative searches. These are searches done for purposes other than law enforcement; for example, for a

fire inspection. Court authorization is required for involuntary administrative searches, although the standards are lower. The only time the government doesn't need a warrant for an administrative search is when they are searching businesses in highly regulated industries such as liquor, guns, strip mining, waste management, nuclear power, etc. This exception to the warrant requirement clearly does not apply to the average homeowner, activist organization or community group.

Privacy tip: Just because they're "inspectors" doesn't mean you have to let them in!

If someone shows up at your home or office claiming to be a fire inspector, building code inspector, or some other non-law enforcement government employee who wants to inspect the premises, you can tell them to come back with a warrant. You don't have to let them in without a warrant!

Exigent circumstances. Exigent circumstances are emergency situations where it would be unreasonable for the police to wait to get a warrant, like if a person is calling for help from inside your house, if the police are chasing a criminal suspect who runs into an office or home, or if evidence will be destroyed if the police do not act immediately.

Privacy tip: Don't get tricked into consenting!

Police could try to get your consent by pressuring you, or making you think that you have to let them in. For example, they may show up at your door claiming that your neighbor saw someone breaking into your home or office, saw a criminal suspect entering the premises, or heard calls for help, and that they need to take a look around. You should never physically interfere if they demand to come in (which they will do if there are indeed exigent circumstances), but no matter what they say or do, keep saying the magic words: "I do not consent to a search."

Plain view. The police can make a warrantless search or seizure if they are lawfully in a position to see and access the evidence, so long as that evidence is obviously incriminating. For example, if the police enter a house with a valid search warrant to search for and seize some stolen electronics and then see a bag of drugs in plain view on the coffee table, they can seize the drugs too, even though the warrant didn't specifically authorize that seizure. Similarly, the police could seize the drugs without a warrant, or look at any other documents or things left in plain view in the house, if there were exigent circumstances that led the police into the house — for example, if a suspect they were chasing ran into the house, or if they heard gunshots from inside. Even a law-abiding citizen who does not have any contraband or evidence that the police

would want to seize may still have sensitive documents in plain view that one would not want the authorities to see.

The plain view exception alone does not allow the police to enter your home or office without a warrant. So, for example, even if the police see evidence through your window, they cannot enter and seize it. However, plain view can combine with other exceptions to allow searches that might otherwise require a warrant. For example, if the person with the bag of drugs in the previous example saw the police looking through his window, then grabbed the bag and ran towards the bathroom as if he was about to flush the evidence down the toilet, that would be an exigent circumstance and the police could enter without a warrant to stop him.

Automobiles. Since cars and other vehicles are mobile, and therefore might not be around later if the police need to go get a warrant, the police can search them without one. They still need probable cause, though, because you do have a privacy interest in your vehicle.

If the police have probable cause, they can search the entire vehicle (including the trunk) and all containers in the vehicle that might contain the object for which they are searching. For example, if the police have probable cause to believe that drugs are in the vehicle, they can search almost any container, but if they have probable cause to believe that a murder suspect is hiding inside the vehicle, they must limit their search to areas where a person can hide.

Also, it's important to know that the "plain view" exception is often applied to cars. That means that the police aren't conducting a search just by looking through your car windows, or even by shining a flashlight in your car. And if they see evidence inside your car, that can then give them probable cause to search the rest of the vehicle under the automobile exception.

Police at the (car) door: What if I get pulled over?

If you are pulled over by a police officer, you may choose to stop somewhere you feel safe, both from traffic and from the officer herself. In other words, you can pull into a lighted gas station, or in front of someone's home or somewhere there are other people present, rather than stopping on a dark road, so long as you indicate to the officer by your driving that you are in fact stopping. You are required to show the officer your license, insurance and registration. Keep your hands where the officer can see them at all times. For example, you can wait to get your documentation out when the officer is standing near your car so that she can watch what you are doing and have no cause to fear that you are going into the glove box for a weapon. Be polite and courteous.

Airport searches. As you certainly know if you've flown recently, the government is allowed to search you and all your luggage for bombs and weapons before you are allowed to board a plane, without a warrant. Always assume that the government will look in your bags when you fly, and pack accordingly.

Border searches. The government has the right to warrantlessly search travelers at the border, including international airports, as part of its traditional power to control the flow of items into and out of the country. The case law distinguishes between "routine" searches, which require no cause, and "non-routine" searches, which require reasonable suspicion, but no warrant. "Non-routine" searches include strip searches, cavity searches, involuntary X-rays and other particularly invasive investigative techniques. Several courts have found that searching the contents of your laptop or other electronic devices is "routine" and doesn't require a warrant or even reasonable suspicion.

One solution to this problem is to bring a blank "traveling" laptop and leave your personal information at home. You could then access the information that you left at home over the internet by using a VPN or other secure method to connect to a server where you've stored the information.

However, bringing a clean laptop means more than simply dragging files into the trash. Deleting files will not remove them from your hard drive. See our software and technology article on secure deletion for details.

Another solution is to use password-based disk encryption to prevent border agents from being able to read your files. The consequences of refusing to disclose a password under those circumstances are difficult to predict with certainty, but non-citizens would face a significant risk of being refused entry to the country. Citizens cannot be refused entry, but could be detained until the border agents decide what to do, which may include seizing your computer.

Stop and frisk searches. The police can stop you on the street and perform a limited "pat-down" search or "frisk" — this means they can feel around your outer clothing for concealed weapons.

The police don't need probable cause to stop and frisk you, but they do at least need to have a reasonable suspicion of criminal activity based on specific facts. This is a very low standard, though, and the courts usually give the police a lot of leeway. For example, if a police officer is

suspicious that you're carrying a concealed weapon based on the shape of a lump under your jacket or the funny way that you're walking, that's usually enough.

If, while patting you down, a police officer feels something that he reasonably believes is a weapon or an illegal item, the officer can reach into your clothes and seize that item.

Search Incident to Lawful Arrest

Search Incident to Arrest (SITA) doctrine is an exception to the general requirement that police obtain a warrant before conducting a search. The purpose of this exception is to protect the officer by locating and seizing any weapons the person has and to prevent the destruction of any evidence on the person. According to the SITA doctrine, if an arrest is valid, officers may conduct a warrantless search of the arrestee and the area and objects in close proximity — i.e. the "grab area" — at about the same time as the arrest.

Officers may also perform inventory searches of the arrested person at the time of the arrest or upon arrival at the jail or other place of detention.

So, the police are allowed to search your clothing and your personal belongings after they've arrested you. They can also search any area nearby where you might conceal a weapon or hide evidence. If you are arrested inside a building, this usually means they can search the room they found you in but not the entire building. If you are arrested while driving, this means they can search inside the car, but not the trunk. But if they impound the car, then they can search the trunk as part of an inventory search. This is another example of the way that multiple exceptions to the warrant requirement can combine to allow the police a lot of leeway to search without going to a judge first.

When searches are delayed until some time after the arrest, courts generally have allowed warrantless searches of the person, including containers the arrestee carries, while rejecting searches of possessions that were within an arrestee's control. These no longer present any danger to the officer or risk of destruction because the arrestee is now in custody.

The question remains whether the SITA doctrine authorizes warrantless searches of the data on cell phones and computers carried by or located near the arrestee. There are very few cases addressing this question. In one case in Kansas, for example, the arresting officer downloaded the memory from the arrestee's cellphone for subsequent search. The court found that this

seizure did not violate the Fourth Amendment because the officer only downloaded the dialed and incoming numbers, and because it was imperative to preserve the evidence given the volatile, easily destroyed, nature of cell phone memory.

In contrast, in another case in California, the court held that a cellphone search was not justified by the SITA doctrine because it was conducted for investigatory reasons rather than out of a concern for officer safety, or to prevent the concealment or destruction of evidence. The officers could seize the phone, and then go obtain a warrant to do any searching of it. The decision rejected the idea that the data searched was not private, in light of the nature and amount of information usually stored on cell phones and laptops.

Police at the door: Arrest warrants

If the police arrive at your home or office with an arrest warrant, go outside, lock the door, and give yourself up. Otherwise, they'll just force their way in and arrest you anyway, and then be able to search nearby. It is better to just go peacefully without giving them an excuse to search inside.

Police at the door: Searches of electronic devices incident to arrest

If you are arrested, the officers are going to seize all the property on your person before you are taken to jail. If you have a cell phone or a laptop, they will take that too. If you are sitting near a cell phone or laptop, they may take those as well. The SITA doctrine may allow police to search the data. It many also allow copying for later search, though this is well beyond what the SITA doctrine's original justification would allow.

You can and should password protect your devices to prevent this potentially unconstitutional privacy invasion. But for much stronger protection, consider protecting your data with file and disk encryption.

Prudent arresting officers will simply secure the devices while they get a warrant. There's nothing you can do to prevent that. Do not try to convince the officers to leave your phone or laptop behind by disavowing ownership. Lying to a police officer can be a crime. Also, prosecutors may use your statements against you later to argue that you do not have the right to challenge even an illegal search or seizure of the device, while still being able to introduce information stored on the device against you.

Subpoenas

Another Powerful Investigative Tool

In addition to search warrants, the government has another very powerful legal tool for getting evidence — the *subpoena*. Subpoenas are legal documents that demand that someone produce

specific documents or appear in court to testify. The subpoena can be directed at you to produce evidence you have about yourself or someone else, or at a third party to produce evidence they have collected about you.

- Subpoenas demand that you produce the requested evidence, or appear in court to testify, at some future time. Search warrants, on the other hand, are served and executed immediately by law enforcement with or without your cooperation.

- Subpoenas, unlike search warrants, can be challenged in court before compliance. If you are the recipient of the subpoena, you can challenge it on the grounds that it is too broad or that it would be unduly burdensome to comply with it. If a judge agrees, then the court may quash the subpoena so you don't have to produce the requested evidence. You may also be able to quash the subpoena if it is seeking legally privileged material, or information that is protected by the First Amendment, such as a political organization's membership list or information to identify an anonymous speaker. If the subpoena is directed to a third party that holds information about you, and you find out about it before compliance, then you can make a motion to quash the subpoena on the grounds of privilege or constitutional rights regardless of whether the third party decides it would otherwise comply. However, you have to do so before the compliance date. Subpoenas that are used to get records about you from third parties sometimes require that you be notified, but usually do not.

- Subpoenas are issued under a much lower standard than the probable cause standard used for search warrants. A subpoena can be used so long as there is any reasonable possibility that the materials or testimony sought will produce information relevant to the general subject of the investigation.

- Subpoenas can be issued in civil or criminal cases and on behalf of government prosecutors or private litigants; often, subpoenas are merely signed by a government employee, a court clerk, or even a private attorney. In contrast, only the government can get a search warrant.

Police at the door: Subpoenas

What should you do if a government agent (or anyone else) shows up with a subpoena?

NOTHING.

Subpoenas are demands that you produce evidence at some time in the future. A subpoena does not give anyone the right to enter or search your home or office, nor does it require you to hand over anything immediately. Even a "subpoena forthwith", which asks for immediate compliance, can not be enforced without first going to a judge.

So, if someone shows up with a subpoena, don't answer any questions, don't invite them in, and don't consent to a search — just take the subpoena, say thank you, close the door and call a lawyer as soon as possible!

Data on the Wire

Electronic Surveillance and Communications Privacy

In this section, you'll learn about what the government can do — technically and legally — when it wants to conduct real-time surveillance of your communications, whether by planting a "bug"

to eavesdrop on your face-to-face conversations, "wiretapping" the content of your phone calls and Internet communications, or using "pen registers" and "trap and trace devices" to track who you communicate with and when. We'll also discuss what steps you can take to defend against this kind of surveillance, with a focus on how to use encryption to protect the privacy of your communications.

What Can the Government Do?

When the government wants to record or monitor your private communications as they happen, it has three basic options, all of which we'll cover in-depth: it can install a hidden microphone or "bug" to eavesdrop on your conversation; it can install a "wiretap" to capture the content of your phone or Internet communications as they happen; or it can install a "pen register" and a "trap and trace device" to capture dialing and routing information indicating who you communicate with and when. In this section, we'll lay out the legal rules for when the government can conduct these types of surveillance, and look at some statistics to help you gauge the risk of having your communications targeted.

Electronic Eavesdropping is Legally Hard for the Government, But Technically Easy

As you learned in the last section, wiretapping is legally difficult for the government: it must obtain a hard-to-get intercept order or "super-warrant" from a court, subject to strict oversight and variety of strong privacy protections. However, wiretapping is typically very technically easy for the government. For example, practically anyone within range of your laptop's wireless signal, including the government, can intercept your wireless Internet communications. Similarly, practically anyone within range of your cell phone's radio signal, including the government, can — with a few hundred bucks to buy the right equipment — eavesdrop on your cell phone conversations.

As far as communications that travel over telecommunications' companies cables and wires rather than (or in addition to) traveling over the air, the government has very sophisticated wiretapping capabilities. For example, using a nationwide surveillance system called "DCSNet" ("DCS" stands for "Digital Collection System") that is tied into key telecommunications switches across the country, FBI agents can from the comfort of their field offices "go up" on a particular phone line and start intercepting or pen-trap tapping wireline phone calls, cellular phone calls, SMS text messages and push-to-talk communications, or start tracking a cell phone's location, at a moment's notice. The government is believed to have similar capabilities when it comes to Internet communications. The extensive and powerful capabilities of the DCSNet, first

uncovered in government documents that EFF obtained in a Freedom of Information Act lawsuit (details at http://www.eff.org/issues/foia/061708CKK), are well-summarized in the Wired.com article "Point, Click...Eavesdrop: How the FBI Wiretap Net Operates".

Using "bugs" to eavesdrop on your oral conversations has also gotten much easier for the government with changes in technology. Most notably, the government now has the technical capability, with the cooperation of your cell phone provider, to convert the microphone on some cell phones or the cell phone in your car's emergency services system into a bug. The government likely also has the ability, with your phone company's help, to open the line on your landline phone and use its microphone as a bug, although we've yet to see any specific cases where such landline phone-based bugging has been used. Finally, the government may even have the capability, using remotely-installed government malware, to turn on the microphone or camera on your computer.

Choosing a Communication Method

Old Ways are Often the Best Ways

Considering the government's broad capability to wiretap communications, there isn't much difference in the technical risk that wiretapping poses to your phone calls versus your emails versus your SMS text messages. However, as described in the last section, there are differences in the legal protections for these modes of communication, and as will be described later in this section, there may be technical steps that you can take — such as encrypting your communications — that may be easier or harder depending on which communications method you choose.

So, when thinking about securing your communications against eavesdropping and wiretapping, your first choice — whether to meet in person, call on the telephone, write an email, or tap out an SMS text or IM message — is also your most important choice. As you'll see below, the least technically sophisticated modes of communication like face-to-face conversations and landline telephone conversations are often the most secure against unwanted eavesdropping, unless you and those you communicate with have mastered how to encrypt your Internet communications.

Face-to-Face Conversations Are the Safest Bet

As shown in the last section, government eavesdropping of your "oral communications" or face-to-face conversations using "bugs" or hidden microphones is very rare: only 20 court orders authorizing oral intercepts were reported in the 2007 wiretap report, compared to 1,998 orders

authorizing wiretapping of "wire communications" or voice communications. In other words, you are 100 times more likely to have your phone conversations tapped than to have your face-to-face conversations "bugged".

Not only are your oral conversations at less risk than your phone conversations, but they also receive the same strong legal protections as your phone conversations. Like your phone calls and unlike your non-voice Internet communications, oral communications that are intercepted in violation of the Wiretap Act are subject to that statute's exclusionary rule, and cannot be used against you as evidence in a criminal trial.

Therefore, face-to-face conversations in private are the most secure method of communicating. Deciding whether to talk face-to-face rather than send an email or make a telephone call becomes a traditional security trade-off: is the inconvenience of having to meet face-to-face worth the security gain? Depending on whom you want to talk to and where they are, that inconvenience could be trivial or it could mean a cross-country trip. If the person you want to communicate with is in the same office or just next door, you may want to choose a private conversation even for communications that aren't particularly sensitive. When it comes to your very most sensitive data, though, that cross-country flight might be worth the trade-off.

Just because the risk of oral interception is very low doesn't mean you shouldn't take technical precautions to reduce that risk, particularly when it comes to very sensitive conversations. Therefore, depending on how convenient it is and how sensitive the conversation is — again, it's a trade-off — you may want to have your conversation in a room that does not contain a landline telephone or a computer with a built-in or attached microphone or camera, and either not carry your cell phone or remove its battery (the microphone on some phones can be activated even when the phone is powered down, unless you remove the battery). Even if your conversation isn't especially sensitive, it doesn't hurt to detach external microphones and cameras from your laptop or cover the lens of attached cameras with a small piece of tape when they aren't in use. It's easy to do, and ensures that remote activation of those mics and cameras is one less thing to worry about.

Learn to Encrypt Your Internet Communications

Always remember that anyone with access to a wire or a computer carrying your communications, or within range of your wireless signal, can intercept your Internet communications with cheap and readily available equipment and software. Lawyers call this

wiretapping, while Internet techies call it "packet sniffing" or "traffic sniffing". The only way to protect your Internet communications against wiretapping by the government or anyone else is by using encryption. Of course, it is true that most encryption systems can be broken with enough effort. However, breaking modern encryption systems usually requires that an adversary find a mistake in the way that the encryption was engineered or used. This often requires large amounts of effort and expense, and means that encryption is usually a *critically* significant defensive measure even when it isn't totally impregnable.

Encryption, unfortunately, isn't always easy to use, so as in other cases, your decision of whether to use it will pose a trade-off: is the inconvenience of using the encryption worth the security benefit?

The occasional inconvenience posed by some encryption systems is counter-balanced by the fact that encryption will protect you against much more than overzealous law enforcement agents. Your Internet communications are vulnerable to a wide range of governmental and private adversaries in addition to law enforcement, whether it's the National Security Agency or a hacker trying to intercept your credit card number, and encryption will help you defend against those adversaries as well.

Also, as described in later sections, encrypting your communications not only protects against wiretapping but can also protect your communications while they are stored with your communications provider. So, for example, even if the government is able to seize your emails from your provider, it won't be able to read them.

Considering all the benefits of encryption, we think that it's usually worth the trade-off, although as always, your mileage may vary depending on your tolerance for inconvience and on how serious you judge the threat of wiretapping to be. In some cases, using encryption may not be inconvenient at all. For example, the OTR encryption system for IM is extremely easy to set up and use; there's little reason not to give it a try. Check out the following articles to learn more about how you can use encryption to protect your internet communications against wiretapping, as well as against traffic analysis using pen-trap taps.

Wi-Fi. Using encryption is especially critical when transmitting your Internet communications over the air using Wi-Fi, since pretty much anyone else in the area that has a wireless-enabled laptop can easily intercept your radio signals. This article will explain how to encrypt the radio signals sent between your laptop and a wireless access point.

Virtual Private Networks (VPNs). Virtual Private Networks or "VPNs" are a potent encryption tool allowing you to "tunnel" communications securely over the Internet.

Web browsers. Some of your web communications can be encrypted to protect against traffic sniffing. Take a look at this article to learn more about HTTPS, the most common web encryption standard, as well as other browser security and privacy tips.

Email and IM. There are a number of powerful tools available for encrypting your emails and your IM messages; take a look at these articles to learn more.

Tor. Tor is free, powerful, encryption-based anonymizing software that offers one of the few methods of defending yourself against traffic analysis using pen-trap taps, and also provides some protection against wiretapping. Visit this article for all the details.

Defend Yourself Against Cell Phone Tracking

As described earlier, the government can use information transmitted by your cellular telephone to track its location in real-time, whether based on what cell phone towers your cell phone is communicating with, or by using the GPS chip included in most cell phones.

Many courts have required the government to obtain a warrant before conducting this type of surveillance, often thanks to briefing by EFF. (For more information on our work in this area, visit EFF's cell tracking page.) However, many other courts have been happy to routinely authorize cell phone tracking without probable cause.

Even more worrisome, the government has the capability to track cell phones without the cell phone provider's assistance using a mobile tracking technology code-named "triggerfish". This technology raises the possibility that the government might bypass the courts altogether. Even if the government does seek a court order before using "triggerfish," though, it will only need to get an easy-to-get pen-trap order rather than a wiretap order based on probable cause.

Put simply, cell phone location tracking is an incredibly powerful surveillance technology that is currently subject to weak technical and legal protections.

Unfortunately, if you want to use your cell phone at all, avoiding the threat of this kind of real-time tracking is nearly impossible. That's because the government can track your cell phone

whenever it's on, even if you aren't making a call. The government can even track some cell phones when they are powered down, unless you have also removed the battery. So, once again, there is a security trade-off: the only way to eliminate the risk of location tracking is to leave the cell phone at home, or remove the battery.

For more information about the privacy risks posed by cell phones, take a look at our article on mobile devices. You may also want to take a look at the advice offered by MobileActive.org in its Primer on Mobile Surveillance.

Using the Telephone is Still the Second Safest Bet

If having an oral conversation is simply too great an inconvenience, the second most secure option — unless you've mastered how to encrypt your internet communications — is to use the phone. *Even though your phone is statistically more likely to be wiretapped than your Internet communications, the phone is still less risky than unencrypted Internet communications.*

This is true for several reasons. First and most important, your phone calls don't generate copies of your communications — once your call is over, the communication disappears forever. Internet communications, on the other hand and as discussed more below, generate copies that make it easier and more likely that someone can find out what you said. The risk of subpoenas to get these copies is much higher than the risk of a phone wiretap. Also, many more potential adversaries have or can gain access to your Internet traffic than to your phone lines.

Also, remember that "wire communications" — that is, voice communications — get more legal protection. If your voice communications are wiretapped in violation of the Wiretap Act, they won't be allowed as evidence; illegally wiretapped Internet communications may still end up in court. That means that investigators have less reason to avoid stretching the law when it comes to your electronic communications.

Speaking generally, just as phone conversations are a safer bet than unencrypted Internet communications, *telephone conversations between landline telephones are a safer bet than telephone conversations that involve a cellular telephone*.

Most obviously, conversations that involve cellular telephones are *technically* much easier to tap than your landline phone conversations — anyone who is in range of a cell phone's radio signal can listen in using a few hundred dollars worth of specialized cell phone interception equipment

(for more discussion of the security threats posed to mobile devices like cell phones, see the article on mobile devices). If you are concerned that government agents may ignore the law and choose to intercept your phone conversations without a wiretap order, intercepting your cell phone's radio signals would be an effective way for them to secretly do so, particularly considering that they do not need to get the assistance of the cell phone provider and that their radio-based interception wouldn't leave any physical trace.

Cell phone conversations may also be more vulnerable *legally* — some courts have held that communications using cordless telephones are not protected by the Fourth Amendment, finding that there is no reasonable expectation of privacy in the radio signal sent between the cordless handset and the base station. The government may similarly consider the radio signal sent between your cell phone and the cell phone company's cell tower to be unprotected by the Fourth Amendment.

Privacy tip: Avoiding phone tap paranoia

Contrary to popular belief, modern phone wiretaps used by the government don't make any noise — no clicks, no hisses, no static, nothing. Don't worry that the government is monitoring you if you happen to hear some unexplained noise on the phone line. You wouldn't believe how often we're told, "I think I'm being wiretapped — I keep hearing clicks!"

What About Phone Calls Using the Internet?

Your "wire communications" or voice communications are subject to stronger legal protections than your other communications, regardless of what communications medium you use. So, for example, whether government agents intercept your landline telephone call, your cellular telephone call, or a telephone call made over the Internet, the Wiretap Act's exclusionary rule will prevent them from using that information as evidence against you in a criminal trial if they didn't get a wiretap order first. In contrast, the statute wouldn't prevent the government from using illegally intercepted "electronic communications" like text messages or emails as evidence.

Therefore, you may want to consider using Voice-over-IP (VoIP) services, which allow you to send live voice communications — basically, phone calls — over the Internet. VoIP may be more private than regular calls for one big reason: it's easier to encrypt your conversation, as encrypting regular phone calls is very difficult and expensive. Unfortunately, there isn't any obviously effective and trustworthy option for encrypted VoIP that we can recommend at the moment. See our article on VoIP for futher details.

Avoid SMS Text Messages If You Can

Text messaging over your cell phone using SMS can be an incredibly quick and convenient way of communicating short messages, but from a privacy perspective, it poses some serious problems.

First, just like your cell phone conversations, SMS text messages sent to and from your cell phone can easily be intercepted over radio with minimal equipment and without any cooperation from the cell phone provider.

Second, just like with your cell phone conversations, it's unclear whether the Fourth Amendment protects the radio signals that carry your SMS messages against interception. This uncertainty increases the possibility that the government may intercept such communications without a probable cause warrant.

Third, and unlike your cell phone calls, SMS messages are "electronic communications" rather than "wire communications," and therefore aren't protected by the Wiretap Act's exclusionary rule. That means the statute would allow the government to use your messages against you in a criminal case, even if they were intercepted without a wiretap order in violation of the statute.

Finally, although the Wiretap Act clearly does require the government to obtain a wiretap order before intercepting SMS messages, just as with any other "electronic communication," we have heard anecdotal reports of the government intercepting SMS messages without wiretap orders, instead using the much-easier-to-obtain pen/trap orders. These reports are bolstered by known cases where the government has obtained the content of stored SMS messages under the lesser standards reserved for non-content communications records.

Putting all these factors together, we currently consider SMS messages to be highly vulnerable to government wiretapping, and recommend reserving that mode of communication for only the most trivial of communications, if you use it at all. The only exception is if you use encryption to protect your SMS messages. For now, SMS encryption software for cell phones is still quite rare, though you can find information about such software for Java-enabled phones here.

Learn to Encrypt Your Internet Communications

Always remember that anyone with access to a wire or a computer carrying your communications, or within range of your wireless signal, can intercept your Internet communications with cheap and readily available equipment and software. Lawyers call this wiretapping, while Internet techies call it "packet sniffing" or "traffic sniffing". The only way to protect your Internet communications against wiretapping by the government or anyone else is by using encryption. Of course, it is true that most encryption systems can be broken with enough effort. However, breaking modern encryption systems usually requires that an adversary find a mistake in the way that the encryption was engineered or used. This often requires large amounts of effort and expense, and means that encryption is usually a *critically* significant defensive measure even when it isn't totally impregnable.

Encryption, unfortunately, isn't always easy to use, so as in other cases, your decision of whether to use it will pose a trade-off: is the inconvenience of using the encryption worth the security benefit?

The occasional inconvenience posed by some encryption systems is counter-balanced by the fact that encryption will protect you against much more than overzealous law enforcement agents. Your Internet communications are vulnerable to a wide range of governmental and private adversaries in addition to law enforcement, whether it's the National Security Agency or a hacker trying to intercept your credit card number, and encryption will help you defend against those adversaries as well.

Also, as described in later sections, encrypting your communications not only protects against wiretapping but can also protect your communications while they are stored with your communications provider. So, for example, even if the government is able to seize your emails from your provider, it won't be able to read them.

Considering all the benefits of encryption, we think that it's usually worth the trade-off, although as always, your mileage may vary depending on your tolerance for inconvience and on how serious you judge the threat of wiretapping to be. In some cases, using encryption may not be inconvenient at all. For example, the OTR encryption system for IM is extremely easy to set up and use; there's little reason not to give it a try. Check out the following articles to learn more about how you can use encryption to protect your internet communications against wiretapping, as well as against traffic analysis using pen-trap taps.

Wi-Fi. Using encryption is especially critical when transmitting your Internet communications over the air using Wi-Fi, since pretty much anyone else in the area that has a wireless-enabled laptop can easily intercept your radio signals. This article will explain how to encrypt the radio signals sent between your laptop and a wireless access point.

Virtual Private Networks (VPNs). Virtual Private Networks or "VPNs" are a potent encryption tool allowing you to "tunnel" communications securely over the Internet.

Web browsers. Some of your web communications can be encrypted to protect against traffic sniffing. Take a look at this article to learn more about HTTPS, the most common web encryption standard, as well as other browser security and privacy tips.

Email and IM. There are a number of powerful tools available for encrypting your emails and your IM messages; take a look at these articles to learn more.

Tor. Tor is free, powerful, encryption-based anonymizing software that offers one of the few methods of defending yourself against traffic analysis using pen-trap taps, and also provides some protection against wiretapping. Visit this article for all the details.

Defend Yourself Against Cell Phone Tracking

As described earlier, the government can use information transmitted by your cellular telephone to track its location in real-time, whether based on what cell phone towers your cell phone is communicating with, or by using the GPS chip included in most cell phones.

Many courts have required the government to obtain a warrant before conducting this type of surveillance, often thanks to briefing by EFF. (For more information on our work in this area, visit EFF's cell tracking page.) However, many other courts have been happy to routinely authorize cell phone tracking without probable cause.

Even more worrisome, the government has the capability to track cell phones without the cell phone provider's assistance using a mobile tracking technology code-named "triggerfish". This technology raises the possibility that the government might bypass the courts altogether. Even if the government does seek a court order before using "triggerfish," though, it will only need to get an easy-to-get pen-trap order rather than a wiretap order based on probable cause.

Put simply, cell phone location tracking is an incredibly powerful surveillance technology that is currently subject to weak technical and legal protections.

Unfortunately, if you want to use your cell phone at all, avoiding the threat of this kind of real-time tracking is nearly impossible. That's because the government can track your cell phone whenever it's on, even if you aren't making a call. The government can even track some cell phones when they are powered down, unless you have also removed the battery. So, once again, there is a security trade-off: the only way to eliminate the risk of location tracking is to leave the cell phone at home, or remove the battery.

For more information about the privacy risks posed by cell phones, take a look at our article on mobile devices. You may also want to take a look at the advice offered by MobileActive.org in its Primer on Mobile Surveillance.

Defend Yourself Against Cell Phone Tracking

As described earlier, the government can use information transmitted by your cellular telephone to track its location in real-time, whether based on what cell phone towers your cell phone is communicating with, or by using the GPS chip included in most cell phones.

Many courts have required the government to obtain a warrant before conducting this type of surveillance, often thanks to briefing by EFF. (For more information on our work in this area, visit EFF's cell tracking page.) However, many other courts have been happy to routinely authorize cell phone tracking without probable cause.

Even more worrisome, the government has the capability to track cell phones without the cell phone provider's assistance using a mobile tracking technology code-named "triggerfish". This technology raises the possibility that the government might bypass the courts altogether. Even if the government does seek a court order before using "triggerfish," though, it will only need to get an easy-to-get pen-trap order rather than a wiretap order based on probable cause.

Put simply, cell phone location tracking is an incredibly powerful surveillance technology that is currently subject to weak technical and legal protections.

Unfortunately, if you want to use your cell phone at all, avoiding the threat of this kind of real-time tracking is nearly impossible. That's because the government can track your cell phone

whenever it's on, even if you aren't making a call. The government can even track some cell phones when they are powered down, unless you have also removed the battery. So, once again, there is a security trade-off: the only way to eliminate the risk of location tracking is to leave the cell phone at home, or remove the battery.

For more information about the privacy risks posed by cell phones, take a look at our article on mobile devices. You may also want to take a look at the advice offered by MobileActive.org in its Primer on Mobile Surveillance.

Summing Up

What You Need to Know

Due to a combination of legal and technical factors, face-to-face conversations and conversations using landline telephones are more secure against government wiretapping than cell phone or Internet communications. Cell phone conversations are more vulnerable both technically and legally, while SMS text messaging appears for now to be very insecure both technically and legally. Cell phones also create the risk of location tracking, and the only way to eliminate that risk entirely is to not carry a cell phone or to remove the battery.

When it comes to Internet communications, using encryption is the only way to defend against wiretapping, whether by the government or anyone else.

When it comes to pen/trap taps, on the other hand, most encryption products won't protect the types of information that the government can get. That information needs to be transmitted in the clear so computers can direct it to the proper recipient. Only anonymizing tools like Tor will protect you from traffic analysis via pen/trap tap.

The SSD Project

Summing Up

What You Need to Know

Due to a combination of legal and technical factors, face-to-face conversations and conversations using landline telephones are more secure against government wiretapping than cell phone or Internet communications. Cell phone conversations are more vulnerable both technically and legally, while SMS text messaging appears for now to be very insecure both technically and legally. Cell phones also create the risk of location tracking, and the only way to eliminate that risk entirely is to not carry a cell phone or to remove the battery.

When it comes to Internet communications, using encryption is the only way to defend against wiretapping, whether by the government or anyone else.

When it comes to pen/trap taps, on the other hand, most encryption products won't protect the types of information that the government can get. That information needs to be transmitted in the clear so computers can direct it to the proper recipient. Only anonymizing tools like Tor will protect you from traffic analysis via pen/trap tap.

Information Stored By Third Parties

Third parties — like your phone company, your Internet service provider, the web sites you visit and interact with or the search engine that you use — regularly collect a great deal of sensitive information about how you use the phone system and the Internet, such as information about who you're calling, who's emailing or IMing you, what web pages you're reading, what you're

searching for online, and more. In addition to those records being compiled about you, there's also data that you choose to store with third parties, like the voicemails you store with you cell phone company or the emails you store with your email provider. In this section, we'll talk about the legal rules that govern when and how law enforcement agents can obtain this kind of information stored by and with third parties. We'll then outline steps that you can take to reduce that risk, by learning how to reduce the amount of information collected about you by third parties, minimize the amount of data you choose to store with third parties, or replace plainly readable data with encrypted versions for storage with third parties.

What Can the Government Do?

In addition to being able to use wiretaps to intercept your communications while they are being transmitted, the government has a variety of ways of getting (1) records about your communications and (2) the content of communications that you have stored with a third party. In particular, the government can get all of the records that your ISP, phone company, or other communications service providers have on you, and the SMS messages, instant messages, emails or voice-mails you've stored with them. However, unlike regular third-party records discussed above, which can be subpoenaed without any notice to you, the records of your communications providers are given some extra protection by the "Stored Communications Act" portion of the "Electronic Communications Privacy Act", or ECPA.

So what can the government get?

Some Records Only Require a Subpoena

Basic Subscriber Information Held by Your Communications Providers Is Available With Just a Subpoena

With a subpoena, the government can obtain from your communications providers what is often called "basic subscriber information." Sometimes, the subpoena will specifically name a person whose information is being sought; other times the government will ask for information regarding a particular phone number, Internet username, email address, or IP address. With such a subpoena, the government can (only) get your:

- Name.
- Address.
- The length of time you've used that phone or Internet company, along with service start date and the types of services you use.

- Phone records. They can get your telephone number, as well as local and long distance telephone connection records — those are records identifying all the phone numbers you've called or have called you, and the time and length of each call.

- Internet records. They can get the times you signed on and off of the service, the length of each session, and the IP address that the ISP assigned to you for each session.

- Information on how you pay your bill, including any credit card or bank account number the ISP or phone company has on file.

The government can get this information with no notice to you at all, and can also get a court order forcing your service provider not to tell you or anyone else.

Other Records Require a Court Order

Other Communications Records Held by Your Communications Providers Require a Court Order

In order to get a communications provider to turn over other records beyond basic subscriber information, the government either has to get a search warrant or a special court order. Sometimes called "D" orders, since they are authorized in subsection (d) of section 2703 of the Stored Communications Act, these court orders are much easier to get than search warrants but harder to get than subpoenas. The government can get this information with no notice to you at all, and can also get a court order forcing your service provider not to tell you or anyone else.

In addition to basic subscriber information, your ISP or email provider may maintain records or "logs" of:

- The email addresses of people you send emails to and receive emails from, the time each email is sent and received, and the size of each email

- The IP addresses of other computers on the Internet that you communicate with, when you communicated with them, and how much data was exchanged

- The web addresses of the web pages that you visit

Which, if any, of the above are logged varies, depending on your particular ISP or email provider's privacy policies and resources. However, just about every ISP will log IP addresses and log-on/off times, and keep those logs for at least a few months.

Cellular phone companies may also keep records of which cell tower your phone communicated with when you were making calls. These cell site tower records can help pinpoint your physical location at points in the past, and are increasingly the target of law enforcement investigations. And although some courts have required the government to obtain a warrant

based on probable cause before obtaining these records, the government's usual practice is to get such records based on the much lower "D" Order standard.

Not All Records are Protected

Records Collected by Search Engines and Other Web Sites May Not Be Protected

In addition to the logs kept by your communications providers, there are also logs kept by the Web sites that you visit. For example, the Apache web server is currently the most widely used web server on the Internet. In its default configuration, it logs the following information about each request it receives from a web browser:

- requesting host name/IP address
- username of requester (rarely present)
- time of request
- first line of request (indicating requested page, plus some parameters)
- success or failure of request
- size of response in bytes
- the previous page viewed by requester (if any)
- the name and version of the web browser used

However, the server could potentially be configured to log anything you or your browser tells it, in addition to the above.

The Stored Communications Act clearly protects records held by companies that offer the public the ability to send and receive communications — phone companies, ISPs, webmail providers, IM providers, bulletin board sites, etc. However, it does not necessarily protect logs held by web sites that don't offer communications service, which is most of them.

This is particularly worrisome when it comes to search engines. The government's position is that logs kept by search engines are not protected by the Stored Communications Act *at all*. Considering that these logs can often be linked back to you — either by your IP address or "cookies," or, if you've registered with other services offered by the search engine, by the information you entered when registering — this potential gap in legal protection represents a serious privacy threat.

Some Content Receives Stronger Protection

Emails, Voicemails, and Other Communications Content Stored by Your Communications Providers Receive Stronger Protection

Compared to the relatively weak protection for non-content records, the law gives some extra protection to communications content that you have stored with (or that is otherwise stored by) communications service providers like your phone company, your ISP, or an email provider like Gmail or Hotmail. Your communications providers cannot disclose your stored communications to the government unless the government satisfies the requirements described below; nor can they disclose your stored communications to anyone other than the government without your permission. There is one notable exception, though, for serious emergencies: if the provider believes in good faith that not immediately disclosing the communications could lead to someone's death or serious injury, they can give them to the government.

Note, however, that these restrictions on the disclosure of your communications only apply to communications providers that offer their services to the public. Even more worrisome, the government doesn't consider businesses or schools and universities that offer their employees and students service to be offering services to the public, and therefore considers them unprotected by the Stored Communications Act. That means they could get communications from those entities with only a subpoena, and maybe even just a polite request if your employee agreement or your school's privacy policy allows it.

Privacy tip: Use communications providers that serve the public!

Don't let some friend with a mail server in his basement handle your email service unless he is very trustworthy — unlike a regular ISP or public web-mail service, there are no legal restrictions on who your friend shares your emails with.

The Stored Communications Act strongly protects communications that have been in 'electronic storage' for 180 days or less, but the government has a very narrow reading of what 'electronic storage' means in the statute. The government doesn't consider already-read or opened incoming communications to be in electronic storage (for example, emails in your inbox that you've already looked at, or voicemails in your voicemail account that you've saved after listening). Nor does the government consider messages in your sent box or messages in your drafts box to be in 'electronic storage.' Under the government's view, here's how your communications are treated under the law:

New unopened communications: If the email or voice-mail messages are unopened or unlistened to, and have been in storage for 180 days or less, the police must get a search warrant. However, you are not notified of the search.

Opened or old communications: If you have opened the stored email or voice-mail messages, or they are unopened and have been stored for more than 180 days, the government can use a special court order — the same "D" orders discussed — or a subpoena to demand your communications. Either way, the government has to give you notice (although, like with sneak & peek search warrants, that notice can sometimes be delayed for a substantial time, and as far as we can tell almost always is delayed). However, the police may still choose to use a search warrant instead of a D order or subpoena, so they don't have to give you notice at all.

Notably, the Ninth Circuit Court of Appeals has disagreed with the government's reading of the law, finding that communications are in electronic storage even after they are opened — meaning that the government needs a warrant to obtain opened messages in storage for 180 days or less.

Privacy tip: Use communications providers based in California

Communications providers in states that are in the Ninth Circuit, such as California, are bound by Ninth Circuit law and therefore are very resistant to providing the government with opened emails that are 180 days old or less without a warrant.

In sum, although the law sometimes requires the government to get a warrant before accessing communications you've stored with your communication provider, it doesn't always. For this reason, storing your communications on your own computer is preferable — the government will almost always need a warrant if it wants to seize and search the files on your computer.

What Can I Do To Protect Myself?

When we were talking about how to defend yourself against subpoenas and search warrants, we said, **"If you don't have it, they can't get it."**

Of course, that's only partially true: if you don't have it, they can't get it *from you*. But that doesn't mean they might not be able to get copies of your communications or detailed records about them from someone else, such as your communications service providers or the people and services that you communicate with. Indeed, as we outlined in the last section, it's much

easier as a legal matter for the government to obtain information from these third parties — often without probable cause or any notice to you.

So, you also need to remember this lesson: **"If someone else has stored it, they can get it."** If you let a third party store your voicemail or email, store your calendar and contacts, back up your computer, or log your communications traffic, that information will be relatively easy for the government to secretly obtain, especially compared to trying it to get it from you directly. So, we'll discuss in this section how to minimize the content that you store with third parties.

We've also asked you to **"encrypt, encrypt, encrypt!"** in the previous sections about protecting data on your computer and while you are communicating. The same holds true when protecting against the government getting your information from other people. Although ideally you will avoid storing sensitive information with third parties, using encryption to protect the data that you do store — such as the emails you store with your provider, or the files you back up online — can provide a strong line of defense. We'll talk in this section about how to do that.

Communications content that you've chosen to store with a service provider isn't the only issue, though. There are also the records that those third parties are creating about your interactions with their services. Practically everything you do online will create records, as will your phone calls. So your best defense is to **think before you communicate:**

- Do you really want the phone company to have a record of this call — who you called, when, and how long you talked?
- Do you really want a copy of this email floating around in the recipient's inbox, or on your or his email provider's system?
- Do you really want your cell phone provider to have a copy of that embarrassing SMS text message?
- Do you really want Google to know that you're searching for *that*?

It may be that the communication is so trivial or the convenience so great that you decide that the risk is worth it. But think about it — seriously consider the security trade-offs and make a decision — before you press "send". We'll give you information in this section that should help you make those decisions.

Another option for minimizing the information that's recorded about you — short of avoiding using a service altogether — is to **protect your anonymity using encryption and anonymous communication tools.** If you want to search Google or browse Amazon without them being able to log information that the government could use to identify you, you'll need to use software such as Tor to hide your IP address, as well as carefully manage your browser's privacy settings. This section will give you the information you need to do that.

Getting Started

Learn What Your Service Providers Store

Most communications service providers and commercial web sites have privacy policies. Read them to find out:

- **What information do they collect?** It may be more than you think. If anyone you do business with doesn't have a privacy policy (or their policy is unclear), you should contact them and ask about what they collect.
- **With whom do they share it?** Most companies will share your information with other companies in their corporate family and with marketers; many companies will sell your data to anyone who wants it. Check to see if they'll let you "opt-out" of sharing your information with other companies.
- **What about the government?** Look in the privacy policy to see under what circumstances they'll hand your information over to the government. Try to do business with companies that will not give your information to the government unless required by law to do so. Also find out whether they will notify you if the government asks for your files, and do business with companies who will always notify you unless prohibited by law from doing so. That way, you can call a lawyer and try to stop the disclosure before it happens.

Consider using activist-friendly, privacy-respecting communications providers that offer free services. The Online Policy Group, for example, offers free web hosting and email list hosting, while Rise Up offers free email (including web-mail), web hosting, and email list hosting. These services have strong privacy policies and will notify you of any governmental or other attempt to seek customer information unless prevented by law. Cable companies that offer Internet access usually also have a policy of notifying you unless they've been gagged — in fact, because of a quirky imbalance in the law, they actually have to notify you if they can, unlike non-cable providers. So, if you're especially worried about the communications records held by your ISP, consider using a cable broadband provider.

Again, Telephone Calls are Your Safest Bet

When it comes to protecting the privacy of communications content stored by your provider, the safest choice is to avoid storing any content with the provider *at all*. Therefore, just as when we were discussing wiretapping, regular old telephone calls have a distinct advantage

over other communications methods: putting aside voicemail, which we'll discuss on the next page, telephone calls *don't create copies*. That means, unless the government goes to the technical and legal trouble of directly wiretapping you (a very low risk, compared to the government trying to obtain stored copies of your communications), or the person you are talking to is so untrustworthy that they would record your conversation without telling you (a rarity, but it does sometimes occur), your telephone call will be safe from prying ears.

As you'll see on the following pages, telephone calls are far preferable to SMS text messages, which providers apparently store for long periods of time, and which are very difficult to encrypt. IM and VOIP are better alternatives, as we'll also discuss, since they can be more easily encrypted, and since instant messages and VOIP call contents are typically not logged by providers. Email is a harder case, since it necessarily creates a range of copies — with providers and with recipients — but as you'll see later, there are a number of steps you can take to make that mode of communication safer, too.

Protecting Your Voicemail

As we explained previously, copies of your communications stored by your phone company such as your voicemail receive very weak legal protection compared to copies of your communications stored in your own home. In particular, after a communication has been stored more than 180 days — or, according to the government's reading of the law, after you've first accessed that stored communication — the government no longer needs to get a warrant before obtaining that communication, and can instead use only a subpoena to the company (usually with no notice to you).

When it comes to your voicemail, this means two things:

- Where possible, use your own answering machine or voicemail system, not the phone company's.
- Where it's not possible to use your own answering machine or voicemail system, such as with your cell phone, you should always delete your voicemails as soon as you listen to them!

Protecting Your Voice Over IP Communications

As best we can tell, providers of Voice Over IP telephone service such as Skype do not record your calls as a matter of routine. So, short of using encryption to protect the confidentiality of your calls there are no special steps that you need to take to ensure that the government can't obtain stored copies of your conversations. Notably, Skype uses encryption by default.

However, as discussed in our VoIP article, the security of Skype's encryption system is still in question. And, as with your regular phone calls, there is always going to be some risk that the person at the end of the line is recording the conversation.

Protecting Your Email Inbox

(and Sent folder, and Drafts folder, and…)

The Stored Communications Act requires the government to obtain a warrant before seizing emails that are in "electronic storage" with your communications provider and are less than 181 days old. However, under the government's interpretation of the term "electronic storage", the emails that arrive in your inbox lose warrant protection under the Stored Communications Act, and are obtainable with nothing more than a subpoena (often with no notice to you) as soon as you've downloaded, opened, or otherwise viewed them. Similarly, the government believes that it can obtain the sent emails and draft emails that you store with your provider with only a subpoena, again often without notice to you; the government doesn't think those sent or draft emails are in "electronic storage" as defined by the statute, either.

EFF is doing it's best to prove the government's interpretation wrong in court, and some courts have already disagreed with the government. Yet as far as we can tell, those court decisions haven't significantly changed the government's behavior and it still routinely obtains opened emails (and sent emails and draft emails) without warrants, regardless of how old they are.

Because of the government's aggressive position, you need to be just as aggressive when it comes to defending your email privacy. As described on the next few pages, the most critical things you can do are:

- **Delete emails from your provider's server as soon as you first access the messages,** and store your sent and draft emails locally in your email client software, rather than with your provider.
- In order to minimize the number of emails stored with your provider — be they received, sent, or draft — **avoid using webmail if at all possible**, or, if you do use a webmail account, avoid the web interface and instead configure your email client software to send and receive emails directly via POP.
- **Encrypt your emails** whenever possible.

Protecting Email: Download and Delete!

The single most powerful step you can take to protect the privacy of your email is to not store it with your email provider. Rather than leave email on your provider's server, you should configure your email software to immediately delete incoming emails from your provider's

server as you download those messages to your computer — and also make sure that your email software is configured to store your draft and sent email on your computer rather than with the provider.

Of course, this is a serious security/convenience trade-off — by fetching your email using the "POP" email protocol and storing all your mail locally, you won't have access to your email from multiple devices like you would if you were using the IMAP protocol or a webmail interface, both of which store all of your mail with the provider. We realize that for some people, particularly those without their own computer, using POP and storing everything locally may not be an option. But if it is an option, and you can effectively function without storing your emails with your provider, we highly recommend doing so. For more, check out our email article.

Don't Use Webmail if You Don't Need It - or POP It.

Webmail poses a serious security trade-off for those concerned about a government adversary.

Webmail is usually free, very easy to use, and super-convenient, especially if you want the ability to access your email from several different computers or mobile devices. However, deleting your email from your provider's servers as soon as you've downloaded — a critical step to protecting your email's privacy against the government — is hard if not impossible to do when you use a webmail service like Gmail or Yahoo! Mail, especially if you want to maintain access to a copy of that email. Since you view your email in your browser rather than downloading it to email client software, the only conveniently accessible copy of your email is going to be the one you store with your provider.

If you take the idea of a government adversary seriously, webmail is a very bad risk. The government is hundreds if not thousands of times more likely to try and obtain your stored email rather than wiretap it. Indeed, the reason that the number of wiretaps on electronic communications is so low is *because* it's so easy to obtain the same information from the provider's storage.

So, if you think that government adversaries may pose a threat to your privacy, **we strongly recommend that you not use webmail for any unencrypted sensitive communications**, unless you simply can't live your life or do your job without an easy-to-access-anywhere inbox. If you really don't need that kind of access and usually access your mail from the same computer, the convenience of webmail probably isn't worth the risk.

If you do use a webmail account, though, one way of mitigating the risk is to avoid using the web interface and instead **download your emails directly to your email client software using POP and immediately delete them from the provider's server**. This option may not be available from all webmail providers, but it is offered by major providers such as Gmail, Microsoft and Yahoo!. You'll lose the convenient access to past messages via the web, and it might not be free, but you'll still have cheap and reliable email service.

Protecting Email: Use Email Encryption When You Can

Using email encryption is a good idea even if you are storing all your email locally, if only to counter the wiretapping threat. But using encryption becomes all the more important if you are storing your email content with your email provider. If the government comes calling on your provider with a subpoena for your stored emails, you'll wish you had learned how to protect those messages with encryption, so visit our email article and learn now!

Protecting Instant Messaging

Major IM service providers like AOL, Yahoo! And Microsoft say that they don't store your IM messages after they are transmitted. We think they are telling the truth, but even so, you should use encryption when IMing, if only because it is so easy to do (see our IM article to find out how).

Gmail's chat, on the other hand, logs all of your IMs by default as a feature and stores them online in your Google account for you to access later. If you use Google Talk or Gmail's chat service, we strongly recommend turning off this feature by going "Off the Record" or "OTR", as Google calls it — so that you aren't storing those transcripts with Google.

If you really need access to past transcripts, log them on your own computer using your IM software's settings (subject, of course, to the data retention policy you established after reading our section on protecting data stored on your computer). However, also keep in mind that many if not most of the people you chat with will be keeping their own logs on their own computer (or in their Google account if using Gchat, unless you've gone "Off the Record").

Protecting SMS

Avoid Texting Sensitive Communications

Major cell phone providers claim that they don't log your SMS text messages except for a very short period of time to ensure delivery (see, *e.g.*, statements from providers in this news story

entitled "Most Text Messages Are Saved Only Briefly", or another article containing similar claims). However, there is reason to doubt these claims: we've seen several cases where SMS messages were disclosed by a provider months or even years after they were originally sent. For example, as USA Today recounts, text messages were subpoenaed in the Kobe Bryant rape case four months after they were sent, despite A&T Wireless' claims that customers' text messages are deleted within 72 hours. According to that story, "How messages in the Bryant case would be available four months later isn't known; most likely they were retrieved from an archival storage system." Considering such incidents, provider-side logging of your SMS text messages must be considered a high risk.

Furthermore, although we think that the Stored Communications Act and the Fourth Amendment require the government in most cases to get a warrant before obtaining your pager or SMS messages from your provider, there are several known cases where it has obtained such messages without warrants under the lower legal standards reserved for non-content records, using only subpoenas.

Not only is there the threat of your provider logging your messages and the government subpoenaing them, but also the near certainty that the phones of the people you are communicating with are logging those messages, adding yet another point of vulnerability. That's in addition to the logs on your own phone, which you should delete regularly based on the data retention policy you developed after reading about "Data Stored on Your Computer." However, keep in mind that with the right forensic tools, investigators will likely be able to recover even those deleted messages if they ever get a hold of your phone, and the secure deletion options for mobile devices are still quite limited.

Finally, although there have been some efforts at coming up with encryption solutions that work for SMS (as described in our mobile devices article), none of those techniques are easily or widely used.

Therefore, given the possibility that your SMS texts are logged by your provider, that the government may be able to obtain those messages from your provider without warrants and without notice to you, and that such messages are hard if not impossible to encrypt, along with the certainty that they will be logged on your phone and the phones of the people you communicate with, we strongly recommend against using SMS for any sensitive communications.

Online Storage of Your Private Data

Online Storage of Your Private Data

There's a lot of talk these days about how convenient it is to store your data in the internet "cloud." Why store your calendar or contacts list or critical documents on one computer, or buy a hard drive to back up your files at home, when you can store them "in the cloud" and access them from anywhere using services like Google Calendar, or Google Docs, or remote backup services that will store copies of all your files for you? Well, here's a reason: the government can easily subpoena that data from those providers, with no notice to you.

As we already described in the "What Can The Government Do?" section, the communications stored by your communications service providers are very weakly protected compared to those you store yourself: after 180 days (or after you've downloaded a copy, according to the DOJ), the government can get those communications with only a subpoena and usually with no notice to you. But the situation is even worse when it comes to data that you store with someone other than your communications provider — so called "remote computing services" (RCSs). Under the Stored Communications Act, the government can obtain data that you send to an RCS for storage or processing with only a subpoena regardless of how old it is, and although the government is supposed to notify you before they do, the law makes it very easy for investigators to delay that notice until after they've gotten your data.

Therefore, storing all that data yourself, on your own computers — without relying on RCSs — is the most legally secure way to handle your private information. If you do choose to store copies of your files online, though, we strongly recommend encrypting those files yourself before you do (visit our article on disk and file encryption to learn how), or using services like IDrive or MozyPro that give you the option of encrypting your files using your own private encryption key.

Protecting Your Search Privacy and Your Web Browsing Activity

The search history you generate when using search engines like Google or Yahoo! reveals incredibly sensitive data about what you look at — or even think of looking at — on the web. These logs may be tied to your identity based on your IP address, the cookie files that the search engine places on your computer, or your account information if you've registered to use the search engine or other services offered by the provider. And as discussed earlier in the "What Can the Government Do?" section, these logs are subject to uncertain legal protections.

Considering the sensitivity of search logs and the questions surrounding their legal status, we highly recommend that you exercise great care to ensure that your identity cannot be linked to your search queries. For an in-depth discussion of how to do that, read EFF's "Six Tips to Protect Your Search Privacy". You should also take a look at our article on browsers to learn more about cookie management and on the anonymizing software Tor to learn more about how to mask your IP address. These same techniques can be used to protect you against logging by any web site you visit, not just search engines, and we recommend that you do use them whenever you visit a web site and don't want that site to log personally-identifying information about you and the pages that you read.

Finally, we recommend avoiding using one online portal for multiple services — *e.g.*, try to avoid using Yahoo! Search *and* Yahoo! Mail, or Google Search *and* Google Reader. Not only are you making it easier for the search provider to identify you by virtue of linking all of your activity to your personalized account, but you are also offering the government a convenient "one-stop shop" opportunity to access a wide range of your personal information at once. Using these "mega-portals" to manage all aspects of your online life might be convenient, but it also creates a single point of failure that raises a serious security risk.

TMI on the Web

Do You Really Want to Publish that Blog Post, Flickr that Picture, or Broadcast that Facebook Status?

The web is a powerful engine of personal expression, giving you a wide variety of online venues to speak your mind and communicate with friends or the public. But before you publish that blog post on MySpace or Blogger, post a picture to a picture-sharing sites like Flickr or Picasa, or broadcast your status on Facebook or using Twitter, think, "Is this really information that you want to expose on the web?" Even if you do now, think about years from now: will you want evidence of this youthful indiscretion or that personal opinion floating around on the web in the future? Remember, you don't have any expectation of privacy in information that you post to the public web, and information that you post now but delete later may still persist, whether on the pages of the friends you communicated with (like your Wall Posts to a friend on Facebook), or in Google's cache of old web pages, or the Internet Archive's library of public web pages.

One way of limiting the risks of posting information about yourself on the web is to use the privacy settings offered by social sharing sites like Flickr or Facebook, with which you can avoid publishing your information to the public web and can define which of your "friends" on the same service are allowed access to your information. However, these settings can sometimes

be confusing and difficult to configure correctly, and it's unclear how robust such privacy protections would be against the attacks of a dedicated hacker. There's also the possibility that an adversary may try to "friend" you using fake information to pose as someone you know or would want to know. (A good rule of thumb is to only become "friends" with people that you know personally, after verifying with them via another means of communication — for example, by emailing them or calling them — to ensure that they are the ones that actually made the request.). Then there's the additional threat of adversaries gaining access to your account information by convincing you to use their "app." Finally, of course, there's always the risk that one of your "friends" will republish to others the information that you thought you had posted privately. So, even if you think you've strictly controlled access to your Facebook profile or Flickr page, you should recognize the significant risk that what you post there might leak out, and act accordingly.

Another option, if you're more interested in sharing information and opinion than in socializing, is to communicate *anonymously*, without tying your posts to your real identity. For an extended discussion of how to do that safely and effectively, take a look at our guide on "How to Blog Safely (About Work or Anything Else)."

Protecting Your Location Information

More on Cell Phone Tracking

We described earlier how the government can enlist your phone company's help in tracking the location of your phone in real time. However, that's not the only location privacy threat posed by your cell phone: your provider also keeps records of where your cell phone was each time you made or received a phone call.

In particular, phone companies typically log the cell phone tower you were closest to when you called someone or someone called you, as well as which "sector" of the tower's coverage area your phone was in. Particularly in urban environments where there are lots of cell towers, such records can locate you with a fairly high degree of precision, sometimes to within a city block or even within a particular building. The government routinely obtains these kinds of location records with only subpoenas and with no notice to the target, although EFF is working hard to ensure that such data can only be obtained with a search warrant.

Unfortunately, there's nothing you can do to prevent these records from being created short of not making phone calls, and turning your phone off to ensure that no one calls you. Indeed, turning your phone off might be your only recourse — particularly since some experts have

advised us that the phone companies not only log the location of your phone when a call is made but also log the closest cell tower *whenever* your phone is turned on, as your phone continuously registers itself with the cell network.

Therefore, as is true with every communications device that you use, your best defense is to *think* before you use your cell phone. Do you *really* want your phone company to have a log reflecting that you were in *that* part of town at *that* time? If not, then you should turn the cell phone off.

Another potential solution is to anonymously purchase a prepaid cell phone using cash. The phone company will still have the same location data, but it won't be as easily linked to your identity. Keep in mind, however, that even if the phone company doesn't have subscriber information like your name and address, investigators might be able to quickly associate you with the phone based on the people you communicate with, or based on security camera footage from the store where you bought the phone.

For more information about the privacy risks posed by cell phones, take a look at our article on mobile devices. You may also want to take a look at the advice offered by MobileActive.org in its Primer on Mobile Surveillance.

Summing Up

Whenever you use technology to communicate, you will necessarily leave traces of your activity with third parties like your phone company, your ISP, or your search engine provider. If a third party has it, the government can get it, often under weak legal standards and without any notice to you. So remember:

- **Think before you communicate.** Do you really want there to be a record of this?
- **Choose to make a telephone call when you can**, rather than using SMS or the Internet, **unless your communications are encrypted**. Otherwise, there may be a record of the content of your communication on some third party's server or in an archival database.
- **Avoid storing your data with third parties when you can.** The records you store with others receive much less legal protection than those you store yourself.
- **Use file encryption where possible** if you do choose to store data with an online service.
- If you are using email or voicemail, **delete the copies stored by your communications provider as soon as you download or listen to them.**

- **Learn how to hide your identity online** and minimize the information that online services log about you by learning how to configure your browser and use anonymizing technologies like Tor.

Powerful new communications technologies carry with them powerful risks to the privacy and security of your communications. Learn to defend yourself!

Foreign Intelligence and Terrorism Investigations

All of the government surveillance tactics and standards discussed in previous sections relate to law enforcement investigations — that is, investigations for the purpose of gathering evidence for criminal prosecution. However, the government also engages in surveillance in order to combat foreign threats to national security. When it comes to foreign spies and terrorists, the government uses essentially the same tools — searches, wiretaps, pen/traps, subpoenas — but operates under much lower legal standards and in much greater secrecy. It's important that you understand these foreign intelligence surveillance authorities such as the government's access to records using National Security Letters and its wiretapping powers under the Foreign Intelligence Surveillance Act (FISA) so that you can evaluate the risk of such surveillance to you or your organization and defend against it.

National Security Letters

Imagine if the FBI could, with only a piece of paper signed by the special agent in charge of your local FBI office, demand detailed information about your private Internet communications directly from your ISP, webmail service, or other communications provider. Imagine that it could do this:

- without court review or approval
- without you being suspected of a crime
- without ever having to tell you that it happened

Further imagine that with this piece of paper, the FBI could see a wide range of private details, including:

- your basic subscriber records, including your true identity and payment information
- your Internet Protocol address and the IP address of every Web server you communicate with
- the identity of anyone using a particular IP address, username, or email address
- the email address or username of everyone you email or IM, or who emails or IMs you

- the time, size in bytes, and duration of each of your communications, and possibly even the web address of every website you visit

Finally, imagine that the FBI could use the same piece of paper to gain access your private credit and financial information — and that your ISP, bank, and any other business from which the FBI gathers your private records is barred by law from notifying you.

Now, stop imagining: the FBI already has this authority, in the form of National Security Letters. These are essentially secret subpoenas that are issued directly by the FBI without any court involvement. Thanks to the USA PATRIOT Act, the only requirement the government must meet to issue an NSL is that the FBI must certify in the letter that the information it is seeking is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities.

The number of National Security Letters used each year is classified, but the Washington Post has reported that by late 2005, the government had on average issued 30,000 National Security Letters each year since the PATRIOT Act passed in 2001. That's a hundredfold increase over the pre-PATRIOT numbers.

Further revelations by the FBI's Inspector General in 2007 showed that in many cases, the FBI had failed even to meet the weak post-PATRIOT National Security Letter standards, illegally issuing so-called "exigent letters" to communications providers asking for the same information National Security Letters are used to obtain, but without meeting the minimal requirement that the requested information be relevant to an authorized terrorism or espionage investigation. EFF has since sued the Department of Justice to learn more about how the government has been abusing its National Security Letter authority.

Surveillance Under the Foreign Intelligence Surveillance Act (FISA)

The History of FISA

As stated above, the government was free to wiretap whenever it wanted to in law enforcement investigations until the Supreme Court addressed the issue in 1967, and Congress passed the Wiretap Act in 1968. Similarly, the legality of warrantless searches and wiretaps in national security investigations, as opposed to law enforcement investigations, wasn't settled until the seventies.

In 1972, the Supreme Court ruled on the use of wiretaps in national security cases. In that case, a group of Americans protesting the Vietnam War tried to blow up their local CIA recruiting office. Investigators collected evidence against them with a wiretap but without getting a wiretap order, and argued in court that since the investigation was for national security, the president had the authority to authorize surveillance without having to go through the courts.

The Supreme Court held that the government didn't have unlimited power to conduct surveillance without the approval of a judge just by claiming the investigation was for national security, at least when investigating domestic threats to national security (that is, threats from U.S. citizens and legal residents). It left open whether or not such warrantless surveillance was allowed when investigating foreign threats.

After this decision, and after revelations throughout the seventies that the government had been engaging in an enormous amount of unauthorized spying during the 1960s and early 1970s, Congress decided to provide a legal framework to rein in foreign intelligence investigations. The Foreign Intelligence Surveillance Act of 1978 (or "FISA"), along with later amendments to that act, created a warrant procedure for foreign intelligence investigations so that there would no longer be any foreign intelligence surveillance without court oversight.

FISA in Action

FISA requires the government to get search warrants and wiretap orders from a court even when it is investigating foreign threats to national security. However, the FISA process is different from the law enforcement processes described in earlier sections.

First, all government requests for foreign intelligence surveillance authorization are made to a secret court: the FISA court. In order to get authorization, a significant purpose of the surveillance must be to gather foreign intelligence information — information about foreign spies, foreign terrorists, and other foreign threats — instead of evidence of a crime.

Most importantly, the probable cause standard is very different. Instead of having to show probable cause that a crime is being, has been, or will be committed, the government must show that the target of the surveillance is a foreign power or an agent of a foreign power.

Also unlike law enforcement surveillance, the target is never told by the government that he/she was spied on, and every person that is served with a FISA search warrant, wiretap or

pen/trap order, or subpoena is also served with a gag order forbidding them from every telling anyone about it except their lawyer.

Foreign Powers and Their Agents. So, what exactly qualifies as a foreign power or agent of a foreign power when it comes to FISA surveillance? It's a bit unclear. The FISA law defines those terms only vaguely, and without any access to the decisions of the secret FISA court, there's no way of telling how broadly or narrowly the definitions are being interpreted.

According to FISA, a Foreign Power is defined to include:

- Any foreign government or component of a foreign government, whether or not officially recognized by the United States
- Any "faction" of a foreign nation or nations, or any foreign-based political organization, that isn't "substantially" composed of United States persons ("faction" and "substantially" aren't defined; a U.S. person is a citizen or a legal resident of the U.S.)
- Any entity, like a political organization or a business, that is directed or controlled by a foreign government
- Any group engaged in, or preparing to engage in, "international terrorism." ("International terrorism" is broadly defined as activities that (1) involve violent acts or acts dangerous to human life that are a violation of U.S. criminal laws or would be a violation if committed in the U.S., (2) appear to be intended to intimidate or coerce a civilian population, to influence the policy of a government by intimidation or coercion, or to affect the conduct of a government by assassination or kidnapping, and (3) occur totally outside the U.S., or transcend national boundaries in terms of how they are accomplished, the people they are intended to coerce or intimidate, or the place where the terrorists operate)

According to FISA, an Agent of a Foreign Power is defined to include:

- Anyone that is not a U.S. person who is an officer or employee of a foreign power
- Anyone that is not a U.S. person who engages in "clandestine intelligence activities" (spying) in the U.S. on behalf of a foreign power or any U.S. person that does the same and may be violating the law. So, if you're not a U.S. person, you don't have to be suspected of a crime; but even if you are a U.S. person, that suspicion doesn't have to meet traditional probable cause standards
- Anyone, whether a U.S. person or not, who engages in or prepares for acts of international terrorism or sabotage

If you think that all sounds like very vague gobbledy-gook, you're right. No one really knows what these terms mean other than the FISA court, which won't release its decisions.

And it's even worse for FISA subpoenas, which can be used to force anyone to hand over anything in complete secrecy, and which were greatly strengthened by Section 215 of the USA PATRIOT Act. The government doesn't have to show probable cause that the target is a foreign power or agent — only that they are seeking the requested records "for" an intelligence or terrorism investigation. Once the government makes this assertion, the court must issue the subpoena.

Police at the door: FISA Orders and National Security Letters

If federal agents serve you with a FISA warrant or subpoena, or a National Security Letter, the advice given for regular warrants and subpoenas applies. However, FISA orders and National Security Letters will also come with a gag order that forbids you from discussing them. Do NOT violate the gag order. Only speak to members of your organization whose participation is necessary to comply with the order, and your lawyer. The constitutionality of FISA orders and especially National Security Letters is a matter of great dispute — in particular, several courts have found that the gag order that comes with a National Security Letter violates the First Amendment — and you may be able to successfully challenge the government's demand in court. If you do decide to seek counsel and do not have an a lawyer of your own, you can call the lawyers at EFF.

FISA Wiretap Statistics

Like law enforcement wiretaps, FISA surveillance is relatively rare. Also like law enforcement wiretaps, however, FISA surveillance probably sweeps in the communications of a great many people. Because the information released about FISA surveillance is so limited, though, it's impossible to gauge just how many people are affected and how many communications are intercepted. The only public data available on FISA are the numbers of applications made to, and approved by, the FISA court. And those numbers have steadily increased through the years, to the point where FISA orders now outnumber all federal and state wiretap orders combined! For example, in 2007, 2,370 applications for FISA wiretaps were granted by the FISA court, compared to 2,208 state and federal wiretaps reported in the same year. And each application can contain a request for more than one type of surveillance — for example, a wiretap, a secret search, and secret subpoenas.

Like with law enforcement wiretaps, your FISA wiretap risk is very low, as is the risk of being subjected to a secret physical search under FISA. The risk of having records about you secretly subpoenaed under FISA is much higher, but if it's your communications records the government is after, they're more likely to use a National Security Letter.

Privacy tip: Foreign Intelligence Surveillance

If your organization deals with lots of non-U.S. persons or any foreign governments or foreign-based organizations, you will likely face a higher risk of foreign intelligence surveillance, and should factor that risk into your security decision-making.

Beyond FISA

The NSA Surveillance Program, the Protect America Act and the FISA Amendments Act

FISA is a dangerously weak restraint on the government's power to secretly spy on Americans without probable cause of a crime, particularly since passage of the USA PATRIOT Act in 2001. Yet just as the Bush Administration was successfully lobbying Congress to expand its FISA surveillance authority through the USA PATRIOT Act, it was already building a new surveillance program at the National Security Agency (NSA) that would secretly ignore FISA's limitations and spy on Americans without first going to the FISA court.

The NSA's Surveillance Program Revealed

In a story published on December 16, 2005, the New York Times first revealed to the country that since 9/11, the NSA had regularly targeted Americans in the U.S. for electronic surveillance without first obtaining the required court orders from the FISA court. The president and his representatives quickly admitted that the Bush administration had chosen to bypass FISA as part of its "Terrorist Surveillance Program" or "TSP." The administration claimed that the TSP was narrowly targeted at international communications — i.e., communications into and out of the country — where at least one of the parties had known links to terrorist organizations. The president made the frighteningly broad claim that because of his inherent power under the Constitution to combat foreign threats as Commander-in-Chief, he had the authority to order such warrantless surveillance regardless of FISA's dictates or the Fourth Amendment.

However, the warrantless surveillance proved to be much broader than the "narrow and targeted" program that the president described. Further reporting by the Times and other papers made clear that the NSA's surveillance program went far beyond the admitted "TSP." Those news stories, along with whistleblower evidence [PDF], demonstrated that the NSA program amounted to an untargeted dragnet of millions of ordinary Americans' domestic communications and communications records. With the cooperation of the country's major telecommunications companies such as AT&T, the NSA had illegally gained backdoor access to critical telecommunications switching facilities and communications records databases around the nation. With that illegal access, the government was vacuuming up all of the data passing through those facilities — not only records of who communicated with whom and when but also

the content of nearly every American's private communications — as part of a vast data-mining program. In response to the mounting evidence of a dragnet surveillance program (view a summary of all of that evidence [PDF]), EFF brought suit against AT&T in 2006 — and later, in 2008, against the government itself — on behalf of ordinary AT&T customers seeking to stop the warrantless surveillance of their telephone and Internet communications. You can find out more about the progress of those lawsuits, Hepting v. AT&T and Jewel v. NSA, at our NSA Multi-District Litigation page.

The Protect America Act of 2007, the FISA Amendments Act of 2008, and the Future of the NSA's Surveillance Program

One might expect that the revelation of a massive and illegal spying program would lead to broad bipartisan condemnation from Congress and an effort to pass legislation to provide additional protections against unbridled Executive spying. Unfortunately, that's not what happened. Instead, the Bush administration was able to use fear of terrorism to convince Congress to pass bills authorizing surveillance programs even broader than the admitted "TSP."

Claiming that critical intelligence about potential terrorist attacks would be lost unless FISA was immediately "modernized," the White House succeeded in convincing Congress to pass two laws. First was the temporary Protect America Act ("PAA") of 2007, which expired after one year. Next was the second and more-permanent FISA Amendments Act ("FAA") of 2008. Both allowed the Executive Branch to target the communications of people outside of the U.S. for surveillance without prior FISA court approval and without demonstrating any link to terrorism. Interpreted aggressively, these statutes arguably authorized the programmatic, non-particularized dragnet surveillance of any American's international communications, opening the door to virtually unchecked executive power to intercept your international emails and telephone calls.

In the meantime, although we don't think that the PAA or the FAA authorizes it, there's been no indication that the domestic dragnet, revealed by news reports and whistleblower evidence and alleged in EFF's lawsuits, has ended. As far as we know, the NSA is still plugged into key telecommunications facilities across the country and acquiring copies of all of the communications content that flows through them, while also obtaining records detailing the communications activity of millions of ordinary Americans, in violation of FISA and the Fourth Amendment.

Considering the latest changes to the law, we strongly recommend encrypting all of your international communications traffic. As for protecting the privacy of your domestic communications, the best way to combat the NSA's unchecked access to the nation's communications infrastructure — short of encrypting every single communication or avoiding using telecommunications at all — is to support EFF in its litigation and lobbying efforts to stop the spying for good.

Summing Up

What You Need to Know

To sum up, the steps you'd take to combat FISA surveillance or national security letters are the same ones you'd take in the law enforcement context:

- If you don't keep it, they can't get it — destroy unnecessary records.
- If you do keep it, protect it with file encryption and strong passwords.
- Encrypt your Internet communications to prevent wiretapping.
- Use anonymizing tools like Tor when you're online.
- Always delete your providers' copies of emails and voicemails as soon as you can access them.