ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Defending Freedom on the Electronic Frontier **eff.org**

Know Your Rights

Your computer, phone, and other digital devices hold vast amounts of personal information about you and your family. This sensitive data is worth protecting from prying eyes, including those of the government.

The Fourth Amendment to the U.S. Constitution protects you from unreasonable government searches and seizures, and this protection extends to your computer and portable devices. But how does this work in the real world? What should you do if the police or other law enforcement officers show up at your door and want to search your computer?

EFF has designed this guide to help you understand your rights if officers try to search the data stored on your computer or portable electronic device, or seize it for further examination somewhere else. Keep in mind that the Fourth Amendment is the minimum standard, and your specific state may have stronger protections.

Because anything you say can be used against you in a criminal or civil case, before speaking to any law enforcement official, you should consult with an attorney. Remember, generally the fact that you assert your rights cannot legally be used against you in court. You can always state: “I do not want to talk to you or answer any questions without my attorney present.” If they continue to ask you questions after that point, you can say: “Please don’t ask me any further questions until my attorney is present.” And if the police violate your rights and conduct an illegal search, often the evidence they obtain as a result of that search can’t be used against you.

We've organized this guide into three sections:

- **Overview: When can the police search my devices?**
- **The police have a warrant. Now what?**
- **The police can't get in to my computer. Now what?**

Overview: When can the police search my devices?

- If you consent to a search, the police don't need a warrant.
- Law enforcement may show up at your door. Apart from a few exceptions, police need a warrant to enter your home.
- Be aware that the police can ask your roommate/guest/spouse/partner for access to your computer if they don't have a warrant.
- Even if you're arrested, police can only search your phone under limited circumstances.
- Police can search your computer or portable devices at the border without a warrant.

If you consent to a search, the police don't need a warrant.

The most frequent way police are able to search is by asking you for permission. If you say "yes" and consent to the search, then police don't need a warrant. You can limit the scope of that consent and even revoke or take it back after the officers begin searching, but by then it may be too late.[1] That's why it's better not consent to a search--police may drop the matter. If not, then they will generally need to get a search warrant to search.

Law enforcement may show up at your door. Apart from a few exceptions, police need a warrant to enter your home.

The police can't simply enter your home to search it or any electronic device inside, like a laptop or cell phone, without a warrant.

When the police knock on your door, you do not have to let them in unless they have in their possession and show you a valid search warrant. The safest thing to do is step outside and shut the door behind you. They may or may not indicate right away why they are there. If they have a warrant, ask to see it. If they offer to simply "interview" you, it is better to decline to speak until your attorney can be present. You can do this by telling the officer: "I do not want to talk to you. I do not consent to a search. I want to speak to my attorney."

There are two major ***exceptions*** to the warrant requirement. First, if you consent to a search, then the police can search within the scope of your consent.[2] That's why it is usually better to not consent to a search.

Second, if police have probable cause to believe there is incriminating evidence in the house or on an electronic device that is under immediate threat of destruction, they can immediately search it without a warrant.[3]

Be aware that the police can ask your roommate/guest/spouse/partner for access to your computer if they don't have a warrant.

The rules around who can consent to a search are fuzzy. The key is who has control over an item. Anyone can consent to a search as long as the officers reasonably believe the third person has control over the thing to be searched.[4] However, the police cannot search if one person with control (for example a spouse) consents, but another individual (the other spouse) with control explicitly refuses.[5] It's unclear, however, whether this rule applies to items like a hard drive placed into someone else's computer.[6] And even where two people have control over an item or place, police can remove the non-consenting person and return to get the other's consent to search.[7]

You may want to share this know your rights guide with everyone in your home and ask them not to consent to a search by law enforcement.

Even if you're arrested, police can only search your phone under limited circumstances.

After a person has been arrested, the police generally may search the items on her person and in her pockets, as well as anything within her immediate control, automatically and without a warrant. But the Supreme Court has ruled that police cannot search the data on a cell phone under this warrant exception.[8] Police can, however, search the physical aspects of the phone (like removing the phone from its case or removing the battery) and in situations where they actually believe evidence on the phone is likely to be immediately destroyed, police can search the cell phone without a warrant.

Police can search your computer or portable devices at the border without a warrant.

Fourth Amendment protection is not as strong at the border as it is in your home or office.[9] This means that law enforcement can inspect your computer or electronic equipment, even if they have no reason to suspect there is anything illegal on it.[10] An international airport, even if many miles from the actual border, is considered the functional equivalent of a border.[11] However, border officials in Alaska, Arizona, California, Guam, Hawaii, Idaho, Montana, Northern Mariana Islands, Oregon and Washington can only confiscate an electronic device and conduct a more thorough "forensic" examination of it if they have reasonable suspicion you've engaged in criminal behavior.[12]

The police have a warrant. Now what?

- Ask to see the warrant.
- The warrant limits what the police can do.
- Although the warrant limits what the police can look for, if they see something illegal while executing a warrant they can take it.
- If the police want to search your computer, it doesn't matter whether you're the subject of their investigation.
- You do not have to assist law enforcement when they are conducting their search.
- You do not have to answer questions while law enforcement is searching.

Ask to see the warrant.

A warrant is a document signed by a judge giving the police permission to either arrest you or search your property and take certain items from that property. You have the right to see the warrant and should check to make sure it is valid.

A warrant should contain:

- The correct name of the person arrested or the correct address of the specific place to be searched;
- A list of the items that can be seized or taken by the police;
- The judge's signature;
- A deadline for when the arrest or search must take place

The police must take the warrant with them when executing it and give you a copy of it.[13] They must also knock and announce their entry before they try to forcefully enter your home,[14] and must serve the warrant during the day in most circumstances.[15]

The warrant limits what the police can do.

The purpose of the warrant is to give the judge, not the police, the discretion to decide what places can be searched and which items can be taken.[16] That's why a warrant is supposed to state exactly what the police can search and seize.[17] However, if the warrant authorizes the police to search for evidence of a particular crime, and such evidence is likely to be found on your computer, some courts have allowed the police to search the computer without a warrant.[18]

And remember, if you consent to a search, it doesn't matter if the police have a warrant; any search is permissible as long as the search is consistent with the scope of your consent.

Although the warrant limits what the police can look for, if they see something illegal while executing a warrant they can take it.

While the police are searching your home, if they observe something in "plain view" that is suspicious or incriminating, they may take it for further examination and can rely on their observation to later get a search warrant.[19] For example, if police see an open laptop with something obviously illegal on the screen, they could seize that laptop.

If the police want to search your computer, it doesn't matter whether you're the subject of their investigation.

It typically doesn't matter whether the police are investigating you, or think there is evidence they want to use against someone else located on your computer. If they have a warrant, if you consent to the search, or they think there is something incriminating on your computer that may be immediately destroyed, the police can search it. But remember, regardless of whether you're the subject of an investigation, you can always seek the assistance of the lawyer.

You do not have to assist law enforcement when they are conducting their search.

You do not have to help the police conduct the search. But you should not physically interfere with them, obstruct the search or try to destroy evidence, since that can lead to your arrest. This is true even if the police don't have a warrant and you do not consent to the search, but the police insist on searching anyway. In that instance, do not interfere but write down the names and badge numbers of the officers and immediately call a lawyer.

You do not have to answer questions while law enforcement is searching.

You do not have to answer any questions. In fact, because anything you say can be used against you and other individuals, it is best to say nothing at all other than "I do not want to talk to you. I do not consent to a search. I want to speak to my attorney." However, if you do decide to answer questions, be sure to tell the truth. In many contexts, it is a crime to lie to a police officer and you may find yourself in more trouble for lying to law enforcement than for whatever it was on your computer they wanted.[20]

The police can't get in to my computer. Now what?

- The police can take your computer with them and search it somewhere else.
- You do not have to hand over your encryption keys or passwords to law enforcement.
- You may be able to get your computer back if it is taken and searched.
- There is less protection against a search at a place of employment.

The police can take your computer with them and search it somewhere else.

As long as the police have a warrant, they can seize the computer and take it somewhere else to search it more thoroughly. As part of that inspection, the police may make a copy of media or other files stored on your computer.[21]

You do not have to hand over your encryption keys or passwords to law enforcement.

The Fifth Amendment protects you from being forced to give the government self-incriminating testimony. Courts have generally accepted that telling the government a password or encryption key is "testimony." A police officer cannot force or threaten you into giving up your password or unlocking your electronic devices. However, a judge or a grand jury may be able to force you to decrypt your devices in some circumstances. Because this is a legally complicated issue, if you find yourself in a situation where the police, a judge or grand jury are demanding you turn over encryption keys or passwords, you should let EFF know right away and seek legal help.

You may be able to get your computer back if it is taken and searched.

If your computer was illegally taken, then you can file a motion with the court to have it returned.[22] If the police believe that evidence of a crime has been found on your computer (such as possessing "digital contraband" like pirated music and movies, or digital images of child pornography), the police can keep the computer as evidence. They may also attempt to keep the computer permanently, a legal process known as forfeiture, but you can challenge forfeiture in court.[23]

There is less protection against a search at a place of employment.

Generally, you have some Fourth Amendment protection in your office or workspace.[24] This means the police need a warrant to search your office and work computer unless one of the exceptions described above apply. But the extent of Fourth

Amendment protection depends on the physical details of your work environment, as well as any employer policies. For example, the police will have difficulty justifying a warrantless search of a private office with doors and a lock and a private computer that you have exclusive access to. On the other hand, if you share a computer with other co-workers, you will have a weaker expectation of privacy in that computer, and thus less Fourth Amendment protection.[25] However, be aware that your employer can consent to a police request to search an office or workspace in your absence.[26] Plus, if you work for a public entity or government agency, no warrant is required to search your computer or office as long as the search is for a non-investigative, work-related matter.[27]

Want to learn more about how to protect yourself from unreasonable government searches and surveillance on your computer or portable electronic devices?

- EFF's newly relaunched Surveillance Self-Defense (SSD)is a guide to defending yourself and your friends from digital surveillance by using encryption tools and developing appropriate privacy and security practices.
- EFF's recently updated Cell Phone Guide for U.S. Protestors explains your rights, and how best to protect the data on your phone, at protests.

Notes:

1. Florida v. Jimeno, 500 U.S. 248, 252 (1991).
2. Schneckloth v. Bustamonte,412 U.S. 218, 219 (1973); United States v. Lopez-Cruz, 730 F.3d 803, 809 (9th Cir. 2013); United States v. Vanvliet, 542 F.3d 259, 264 (1st Cir. 2008).
3. Ker v. California, 374 U.S. 23, 39 (1963).
4. Illinois v. Rodriguez, 497 U.S. 177, 181 (1990); United States v. Stabile, 633 F.3d 219, 230-31 (3d Cir. 2011); United States v. Andrus, 483 F.3d 711, 716 (10th Cir. 2007).
5. Georgia v. Randolph, 547 U.S. 103, 106 (2006).
6. United States v. King, 604 F.3d 125, 137 (3d Cir. 2010).
7. Fernandez v. California, 134 S.Ct. 1126, 1134 (2014).
8. Riley v. California, 134 S.Ct. 2473, 2493 (2014).
9. United States v. Flores-Montano, 541 U.S. 149, 152-53 (2004).
10. United States v. Arnold, 533 F.3d 1003, 1009 (9th Cir. 2008); United States v. Ickes, 393 F.3d 501, 507 (4th Cir. 2005).
11. Almeida-Sanchez v. United States, 413 U.S. 266, 273 (1973); Arnold, 533 F.3d at 1006 (9th Cir. 2008); United States v. Romm, 455 F.3d 990, 996 (9th Cir. 2006); United States v. Roberts, 274 F.3d 1007, 1011 (5th Cir. 2001).
12. United States v. Cotterman, 709 F.3d 952, 957 (9th Cir. 2013)(en banc).
13. Federal Rule of Criminal Procedure 41(f)(1)(C).
14. Wilson v. Arkansas, 514 U.S. 927, 929 (1995).
15. Federal Rule of Criminal Procedure 41(e)(2)(A)(ii).
16. Marron v. United States, 275 U.S. 192, 196 (1927).
17. Andresen v. Maryland, 427 U.S. 463, 480 (1976).
18. United States v. Mann, 592 F.3d 779, 786 (7th Cir. 2010); Brown v. City of Fort Wayne, 752 F.Supp.2d 925, 939 (N.D. Ind. 2010).
19. Horton v. California, 496 U.S. 128, 133 (1990); United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001); United States v. Carey, 172 F.3d 1268, 1272 (10th Cir. 1999).
20. Compare 18 U.S.C. § 1001(a) (maximum punishment for first offense of lying to federal officer is 5 or 8 years) with 18 U.S.C. §§ 1030(a)(2) and (c)(2)(A) (maximum punishment for first offense of exceeding authorized computer access is 1 year).
21. United States v. Hill, 459 F.3d 966, 974 (9th Cir. 2006); In re Search of 3817 W. West End, First Floor Chicago, Illinois 60621, 321 F.Supp.2d 953, 958 (N.D. Ill. 2004); see also Federal Rule of Criminal Procedure 41(e)(2)(B).
22. Federal Rule of Criminal Procedure 41(g).
23. See 18 U.S.C. §§ 982, 983; Federal Rule of Criminal Procedure 32.2.
24. Mancusi v. DeForte, 392 U.S. 364, 369 (1968); United States v. Ziegler, 474 F.3d 1184, 1189 (9th Cir. 2007).
25. Schowengerdt v. United States, 944 F.2d 483, 488-89 (9th Cir. 1991).
26. Ziegler, 474 F.3d at 1191.
27. City of Ontario v. Quon, 560 U.S. 746, 748 (2010); O'Connor v. Ortega, 480 U.S. 709, 722 (1987).