Know Your Rights!

By Hanni Fakhoury, EFF Staff Attorney

June 2011

ELECTRONIC FRONTIER FOUNDATION
eff.org

Know Your Rights!

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

The Fourth Amendment to the 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.

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.

Q: Can the police enter my home to search my computer or portable device, like a laptop or cell phone?

A: No, in most instances, unless they have a warrant. But there are two major exceptions: (1) you consent to the search;[1] or (2) the police have probable cause to believe there is incriminating evidence on the computer that is under immediate threat of destruction. [2]

Q: What if the police have a search warrant to enter my home, but not to search my computer? Can they search it then?

A: No, typically, because a search warrant only allows the police to search the area or items described in the warrant.[3] But 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.[4] Additionally, while the police are searching your home, if they observe something in plain view on the computer that is suspicious or incriminating, they may take it for further examination and can rely on their observations to later get a search warrant.[5] And of course, if you consent, any search of your computer is permissible.

Q: Can my roommate/guest/spouse/partner allow the police access to my computer?

A: Maybe. A third party can consent to a search as long as the officers reasonably believe the third person has control over the thing to be searched.[6] However, the police cannot search if one person with control (for example a spouse) consents, but another individual (the other spouse) with control does not.[7] One court, however, has said that this rule applies only to a residence, and not personal property, such as a hard drive placed into someone else's computer.[8]

Q: What if the police want to search my computer, but I'm not the subject of their investigation?

A: It typically does not 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, 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. Regardless of whether you're the subject of an investigation, you can always seek the assistance of a lawyer.

Q: Can I see the warrant?

A: Yes. The police must take the warrant with them when executing it and give you a copy of it.[9] They must also knock and announce their entry before entering your home[10] and must serve the warrant during the day in most circumstances.[11]

Q: Can the police take my computer with them and search it somewhere else?

A: Yes. 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.[12]

Q: Do I have to cooperate with them when they are searching?

A: No, 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.

Q: Do I have to answer their questions while they are searching my home without a warrant?

A: No, 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 until you have a chance to talk to a lawyer. However, if you do decide to answer questions, be sure to tell the truth. 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 they wanted on your computer.[13]

Q: If the police ask for my encryption keys or passwords, do I have to turn them over?

A: No. The police can't force you to divulge anything. However, a judge or a grand jury may be able to. The Fifth Amendment protects you from being forced to give the government self-incriminating testimony. If turning over an encryption key or password triggers this right, not even a court can force you to divulge the information. But whether that right is triggered is a difficult question to answer. If turning over an encryption key or password will reveal to the government information it does not have (such as demonstrating that you have control over files on a computer), there is a strong argument that the Fifth Amendment protects you.[14] If, however, turning over passwords and encryption keys will not incriminate you, then the Fifth Amendment does not protect you. Moreover, even if you have a Fifth Amendment right that protects your encryption keys or passwords, a grand jury or judge may still order

you to disclose your data in an unencrypted format under certain circumstances.[15] If you find yourself in a situation where the police are demanding that you turn over encryption keys or passwords, let EFF know.

Q: If my computer is taken and searched, can I get it back?

A: Perhaps. If your computer was illegally seized, then you can file a motion with the court to have the property returned.[16] If the police believe that evidence of a crime has been found on your computer (such as "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 make you forfeit the computer, but you can challenge that in court.[17]

Q: What about my work computer?

A: It depends. Generally, you have some Fourth Amendment protection in your office or workspace.[18] This means the police need a warrant to search your office and work computer unless one of the exceptions described above applies. 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.[19] However, be aware that your employer can consent to a police request to search an office or workspace.[20] Moreover, 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.[21]

Q: I've been arrested. Can the police search my cell phone without a warrant?

A: Maybe. 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.[22] This means that the police can physically take your cell phone and anything else in your pockets. Some courts go one step further and allow the police to search the *contents* of your cell phone, like text messages, call logs, emails, and other data stored on your phone, without a warrant.[23] Other courts disagree, and require the police to seek a warrant.[24] It depends on the circumstances and where you live.

Q: The police pulled me over while I was driving. Can they search my cell phone?

A: Maybe. If the police believe there is probably evidence of a crime in your car, they may search areas within a driver or passenger's reach where they believe they might find it - like the glove box, center console, and other "containers."[25] Some courts have found cell phones to be "containers" that police may search without a warrant.[26]

Q: Can the police search my computer or portable devices at the border without a warrant?

A: Yes. So far, courts have ruled that almost any search at the border is "reasonable" - so government agents don't need to get a warrant. This means that officials can inspect your computer or electronic equipment, even if they have no reason to suspect there is anything illegal on

it.[27] An international airport may be considered the functional equivalent of a border, even if it is many miles from the actual border.[28]

Q: Can the police take my electronic device away from the border or airport for further examination without a warrant?

A: At least one federal court has said **yes,** they can send it elsewhere for further inspection if necessary.[29] Even though you may be permitted to enter the country, your computer or portable device may not be.

Want to learn how to protect yourself from unreasonable government snooping on your computer or portable electronic devices?

Then be sure to check out EFF's Surveillance Self-Defense Guide: ssd.eff.org.

Endnotes

1. *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973); *United States v. Vanvilet*, 542 F.3d 259 (1st Cir. 2008).
2. *Ker v. California*, 374 U.S. 23 (1963); *see also United States v. Vallimont*, 378 Fed.Appx. 972 (11th Cir. 2010) (unpublished); *United States v. Smith*, 2010 WL 1949364 (9th Cir. 2010) (unpublished).
3. *See Maryland v. Garrison*, 480 U.S. 79, 84-85 (1987) (citing cases).
4. *See e.g., United States v. Mann*, 592 F.3d 779 (7th Cir. 2010); *see also Brown v. City of Fort Wayne*, 752 F.Supp.2d 925 (N.D. Ind. 2010).
5. *Horton v. California*, 496 U.S. 128 (1990); *see also United States v. Walser*, 275 F.3d 981 (10th Cir. 2001); *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999).
6. *Illinois v. Rodriguez*, 497 U.S. 177 (1990); *United States v. Stabile*, 633 F.3d 219 (3d Cir. 2011); *United States v. Andrus*, 483 F.3d 711 (10th Cir. 2007).
7. *Georgia v. Randolph*, 547 U.S. 103 (2006).
8. *United States v. King*, 604 F.3d 125 (3d Cir. 2010) (court approved search and seizure where two housemates shared a desktop computer, and one housemate granted the police access to the entire computer over the other housemate's objections, even though the objecting housemate was the sole owner of a hard drive in the computer).
9. Federal Rule of Criminal Procedure 41(f)(1)(C).
10. *Wilson v. Arkansas*, 514 U.S. 927 (1995).
11. Federal Rule of Criminal Procedure 41(e)(2)(A)(ii).
12. *See e.g., United States v. Hill*, 459 F.3d 966 (9th Cir. 2006); *In re Search of 3817 W. West End, First Floor Chicago, Illinois 60621*, 321 F.Supp.2d 953 (N.D. Ill. 2004); *see also* Federal Rule of Criminal Procedure 41(e)(2)(B).
13. 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 simply exceeding authorized computer access is generally 1 year).
14. *See United States v. Kirschner*, 2010 WL 1257355 (E.D. Mich. Mar. 30, 2010) (unpublished) (relying on *United States v. Hubbell*, 530 U.S. 27 (2000)).
15. *See e.g., United States v. Hatfield*, 2010 WL 1423103 (E.D.N.Y. April 7, 2010) (unpublished); *In re Boucher*, 2009 WL 424718 (D. Vt. Feb. 19, 2009) (unpublished).
16. Federal Rule of Criminal Procedure 41(g).
17. *See* 18 U.S.C. § 983, Federal Rule of Criminal Procedure 32.2.
18. *Mancusi v. DeForte*, 392 U.S. 364 (1968); *United States v. Ziegler*, 474 F.3d 1184 (9th Cir. 2007).
19. *See e.g., Schowengerdt v. United States*, 944 F.2d 483 (9th Cir. 1991).
20. *See Ziegler*, 474 F.3d at 1191 (citing *Mancusi*).
21. *City of Ontario v. Quon*, 130 S.Ct. 2619 (2010); *O'Connor v. Ortega*, 480 U.S. 709 (1987).
22. *Chimel v. California*, 395 U.S. 752 (1969).
23. *See e.g., United States v. Murphy*, 552 F.3d 405 (4th Cir. 2009); *United States v. Wurie*, 612 F.Supp.2d 104 (D. Mass. 2009); *People v. Diaz*, 51 Cal.4th 84, 244 P.3d 501 (2011).
24. *See e.g., United States v. Wall*, 2008 WL 5381412 (S.D.Fla. Dec. 22, 2008) (unpublished); *United States v. Park*, 2007 WL 1521573 (N.D. Cal. May 23, 2007) (unpublished); *State v. Smith*, 124 Ohio St.3d 163, 920 N.E.2d 949 (2009).
25. *Arizona v. Gant*, 129 S.Ct. 1710 (2009).
26. *See e.g., United States v. Finley*, 477 F.3d 250 (5th Cir. 2007); *Wurie*, 612 F.Supp.2d at 109-110; *United States v. Cole*, 2010 WL 3210963 (N.D.Ga. Aug. 11, 2010) (unpublished); *United States v. McCray*, 2009 WL 29607 (S.D.Ga. Jan. 5, 2009) (unpublished).
27. *United States v. Flores-Montano*, 541 U.S. 149 (2004); *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005).
28. *Almeida-Sanchez v. United States*, 413 U.S. 266, 273 (1973); *United States v. Arnold*, 533 F.3d 1003 (9th Cir. 2008); *United States v. Romm*, 455 F.3d 990 (9th Cir. 2006); *United States v. Roberts*, 274 F.3d 1007 (5th Cir. 2001).
29. *United States v. Cotterman*, 637 F.3d 1068 (9th Cir. 2011).