



FAQ: Wi-Fi mooching and the law

By Declan McCullagh

http://news.com.com/FAQ+Wi-Fi+mooching+and+the+law/2100-7351_3-5778822.html

Story last modified Tue Oct 04 12:08:08 PDT 2005

The recent arrest of a Florida man on charges of unauthorized use of a wireless network could set legal ground rules for open Wi-Fi access.

A man sitting in a Chevy Blazer in a residential neighborhood reportedly was [poking around](#) nearby wireless networks in violation of computer crime laws, according to local police.

This appears to be the first arrest in which the sole offense was allegedly accessing a wireless network without prior authorization, and it's already being viewed as a probable test case. CNET News.com interviewed legal scholars to ask what rules apply to Wi-Fi (also called 802.1x) hot spots.

Is it legal to use someone's Wi-Fi connection to browse the Web if they haven't put a password on it?

Nobody really knows. "It's a totally open question in the law," says [Neal Katyal](#), a professor of criminal law at Georgetown University. "There are arguments on both sides."

Wi-Fi roundup

[Wi-Fi's urban push](#) ▶

Cities take on big Wi-Fi projects--and face challenges to their plans.

That doesn't make much sense. Is there a specific law that regulates Wi-Fi access?

Sort of. The primary law is the federal [Computer Fraud and Abuse Act](#).

You can read it for yourself, but the important part (check out paragraph (a)(2)) covers anyone who "intentionally accesses a computer without authorization or exceeds authorized access." Nobody knows exactly what that means in terms of wireless connections. The law was written in 1986 to punish computer hacking--and nobody contemplated 802.1x wireless links back then.

What do prosecutors think?

We asked the U.S. Justice Department on Thursday. A department representative who did not want to be quoted by name said, essentially, that it depends on the details of each case.

The representative said in an e-mail exchange: "Whether access is considered authorized can be determined in part by the precise circumstances of access, just as it would be in the physical world. The prosecutor and jury would look at how the access was accomplished and what was done with the access before definitively determining that it was unauthorized." In other words, the representative said, someone sitting in a company's parking lot at 3 a.m. for the sole purpose of network connectivity might be viewed as a lawbreaker.

Will we ever get a straight answer?

Yes, but expect it to take a while. "This is a problem with the way the legal system works," says Orin Kerr, a law professor at George Washington University who has written a [detailed article](#) on unauthorized network access. "Nobody knows how an ambiguous law works until a prosecution is brought and a court decides."

Alternatively, Congress could rewrite the Computer Fraud and Abuse Act to clear things up, but nobody expects this to happen anytime soon.

How about sharing? Is it legal for me to share my cable modem or DSL connection with my neighbors?

In many cases the answer is no. It depends on the wording of your contract with your broadband provider. Many don't want you to share. As far back as 2002, Time Warner Cable was [sending warnings](#) to customers with open Wi-Fi access points, and a year later it [sued](#) an apartment complex on charges of illicit sharing. Also, AT&T Broadband [has acknowledged](#) monitoring customers for "inordinately high" usage.

"Our terms of service for Verizon Online DSL customers do prohibit them from sharing their connection," says Verizon spokeswoman Bobbi Henson. "The service is meant for use in one location, which would be their home."

Henson adds: "We haven't seen a lot of problems with this, to tell you the truth. Because of the way the DSL network is configured (with one line into each house), sharing doesn't cause us the network problems, frankly, that it can cause for cable. If we were to receive some kind of complaint, like maybe a neighbor calls and says, 'I know my neighbor is sharing my connection and it's making me mad because other neighbors are getting it for free,' we might warn that customer."

Do all broadband providers feel the same way?

No. DSL provider Speakeasy, for example, doesn't mind wireless sharing. Its [policy](#) says: "Speakeasy believes that shared wireless networks are in keeping with our core values of disseminating knowledge, access to information and fostering community..."

Should I put a password on my Wi-Fi access point at home?

It depends on your own security preferences. If your home computer is properly secured and you're not using your wireless connection for anything sensitive, the biggest reason for adding a password is to prevent strangers from leeching off of your connection.

Not everyone uses a password. Some people think it's more social to have an open access point. [Rob Carlson](#), a system administrator in Baltimore has had an open Wi-Fi access point named "public" at his home for years. "Having a router firewall up in front of your connection is probably a vast improvement (over a direct connection to a cable modem or DSL modem) even if the wireless portion is wide open," Carlson says.

What happens if someone does something unsavory with my Wi-Fi connection? Can I get in trouble?

This is another area of ambiguity. "I don't think you would ever be held vicariously liable for unwittingly allowing someone to use your network even if they're trafficking in [child pornography](#). You're just considered a victim in that case," says [Christian Genetski](#), an information security lawyer at Sonnenschein, Nath and Rosenthal. "It'd be different if you set up your own open relay server and looked the other way while spammers sent billions of messages through your open relay, and you were put on notice and did nothing to stop it."

Still, one reason to tighten up your Wi-Fi security is that an open wireless connection can be used for mischief. In September, a California man [pleaded guilty](#) to spamming people through open Wi-Fi hot spots.

Are state laws about unauthorized access different?

Yes, but often not in an important way. Genetski says that "as a general rule, most states model their computer crime laws after (the federal law)."

If I want to make sure that my Wi-Fi network at home is secure, what should I do?

Our sister site, CNET Reviews, has published a [how-to guide](#) on setting up a Wi-Fi network. Check out the section on security.

CNET News.com's Anne Broache contributed to this report

[Copyright](#) ©1995-2006 CNET Networks, Inc. All rights reserved.