10 ways you might be breaking the law with your computer

Version 1.0
May 16, 2008

By Debra Littlejohn Shinder, MCSE, MVP

For many years, the Internet was the "final frontier," operating largely unregulated—in part because of the jurisdictional nightmare involved in trying to enforce laws when communications crossed not just state lines but also national boundaries. That was then; this is now, and legislation that affects the use of Internet-connected computers is springing up everywhere at the local, state, and federal levels. You might be violating one of them without even knowing it.

In this article, we'll take a look at some of the existing laws and some of the pending legislation that may affect how we use our computers and the Internet. Nothing in this article should be construed as legal advice; this is merely an overview of some of the legislation that's out there, how it has been interpreted by the courts (if applicable), and possible implications for computer users.

1 Digital Millennium Copyright Act (DMCA)

Most computer users have heard of this law, which was signed in 1998 by President Clinton, implementing two World Intellectual Property Organization (WIPO) treaties. The DMCA makes it a criminal offense to circumvent any kind of technological copy protection -- even if you don't violate anyone's copyright in doing so. In other words, simply disabling the copy protection is a federal crime.

There are some exemptions, such as circumventing copy protection of programs that are in an obsolete format for the purpose of archiving or preservation. But in most cases, using any sort of anti-DRM program is illegal. This applies to all sorts of copy-protected files, including music, movies, and software. You can read a summary of the DMCA at http://www.copyright.gov/legislation/dmca.pdf.

If you're a techie who likes the challenge of trying to "crack"DRM," be aware that doing so—*even if you don't make or distribute illegal copies of the copyrighted material* -- is against the law.

2 No Electronic Theft (NET) Act

This is another U.S. federal law that was passed during the Clinton administration. Prior to this act, copyright violations were generally treated as civil matters and could not be prosecuted criminally unless it was done for commercial purposes. The NET Act made copyright infringement itself a federal criminal offense, regardless of whether you circumvent copy-protection technology or whether you derive any commercial benefit or monetary gain. Thus, just making a copy of a copyrighted work for a friend now makes you subject to up to five years in prison and/or up to $250,000 in fines. This is the law referred to in the familiar "FBI Warning" that appears at the beginning of most DVD movies. You can read more about the NET Act at http://www.gseis.ucla.edu/iclp/hr2265.html.

Many people who consider themselves upstanding citizens and who would never post music and movies to a P2P site think nothing of burning a copy of a song or TV show for a friend. Unfortunately, by the letter of the law, the latter is just as illegal as the former.

3 Court rulings regarding border searches

Most Americans are aware of the protections afforded by the U.S. Constitution's fourth amendment against unreasonable searches and seizures. In general, this means that the government cannot search your person, home, vehicle, or computer without *probable cause* to believe that you've engaged in some criminal act.

What many don't know is that there are quite a few circumstances that the Courts, over the years, have deemed to be exempt from this requirement. One of those occurs when you enter the United States at the border. In April of this year, the Ninth Circuit Court of Appeals upheld the right of Customs officers to search laptops and other digital devices at the border (the definition of which extends to any international airport when you are coming into the country) without probable cause or even the lesser standard of *reasonable suspicion.* The Electronic Frontier Foundation (EFF) and other groups strongly disagree with the ruling. You can read more on the EFF Web site (http://www.eff.org/deeplinks/2008/04/no-cause-needed-search-laptops-border).

Meanwhile, be aware that even though you've done nothing illegal and are not even suspected of such, the entire contents of your portable computer, PDA, or smart phone can be accessed by government agents when you enter the United States. So if you have anything on your hard drive that might be embarrassing, you might want to delete it before crossing the border.

4 State laws regarding access to networks

Many states have criminal laws that prohibit accessing any computer or network without the owner's permission. For example, in Texas, the statute is Penal Code section 33.02, Breach of Computer Security. It says, "A person commits an offense if the person knowingly accesses a computer, computer network or computer system without the effective consent of the owner." The penalty grade ranges from misdemeanor to first degree felony (which is the same grade as murder), depending on whether the person obtains benefit, harms or defrauds someone, or alters, damages, or deletes files.

The wording of most such laws encompasses connecting to a wireless network without explicit permission, even if the wi-fi network is unsecured. The inclusion of the culpable mental state of "knowing" as an element of the offense means that if your computer automatically connects to your neighbor's wireless network instead of your own and you aren't aware of it, you haven't committed a crime -- but if you decide to hop onto the nearest unencrypted wi-fi network to surf the Internet, knowing full well that it doesn't belong to you and no one has given you permission, you could be prosecuted under these laws.

A Michigan man was arrested (http://arstechnica.com/news.ars/post/20070522-michigan-man-arrested-for-using-cafes-free-wifi-from-his-car.html) for using a café's wi-fi network (which was reserved for customers) from his car in 2007. Similar arrests have been made in Florida, Illinois, Washington, and Alaska. See

5 "Tools of a crime" laws

Some states have laws that make it a crime to possess a "criminal instrument" or the "tool of a crime." Depending on the wording of the law, this can be construed to mean any device that is designed or adapted for use in the commission of an offense. This means you could be arrested and prosecuted, for example, for constructing a high gain wireless antenna for the purpose of tapping into someone else's wi-fi network, even if you never did in fact access a network. Several years ago, a California sheriff's deputy made the news when he declared "Pringles can antennas" illegal (http://www.engadget.com/2005/07/25/wifi-cantennas-now-illegal/) under such a statute.

6 "Cyberstalking" laws

Stalking is a serious crime and certainly all of us are in favor of laws that punish stalkers. As Internet connectivity has become ubiquitous, legislatures have recognized that it's possible to stalk someone from afar using modern technology. Some of the "cyberstalking" laws enacted by the states, however, contain some pretty broad language.

The Arkansas law (http://www.arkleg.state.ar.us/NXT/gateway.dll?f=templates&fn=default.htm&vid=blr:code), for example, contains a section titled "Unlawful computerized communications" that makes it a crime to send a message via e-mail or other computerized communication system (Instant Messenger, Web chat, IRC, etc.) that uses obscene, lewd, or profane language, with the intent to frighten, intimidate, threaten, abuse, or harass another person. Some of the lively discussions on mailing lists and Web boards that deteriorate into flame wars could easily fall under that definition. Or how about the furious e-mail letter you sent to the company that refused to refund your money for the shoddy product you bought?

Closely related are the laws against "cyber bullying" (http://www.cio-today.com/news/Teen-Suicide-Spurs-Cyberbullying-Law/story.xhtml?story_id=12000B111K60) that have recently been passed by some states and local governments.

The best policy is to watch your language when sending any type of electronic communications. Not only can a loss of temper when you're online come back to embarrass you, it could possibly get you thrown in jail.

7 Internet gambling laws

Like to play poker online or bet on the horse races from the comfort of your home? The federal Unlawful Internet Gambling Enforcement Act of 2006 criminalizes acceptance of funds from bett0ors -- but what about the bettors themselves? Are they committing a crime?

Under this federal law (http://www.gambling-law-us.com/Federal-Laws/internet-gambling-ban.htm), the answer is no, but some state laws do apply to the person placing the bet. For example, a Washington law passed in 2006 (http://seattletimes.nwsource.com/html/localnews/2004418390_gambling16m.html) makes gambling on the Internet a felony. The King County Superior Court just recently upheld that law, although challengers have vowed to take it to the Supreme Court.

Be sure to check out the state and local laws before you make that friendly online bet.

8 Security Breach Disclosure laws

A California law passed in 2003 (http://www.dmv.ca.gov/pubs/vctop/appndxa/civil/civ1798_82.htm) requires that any company that does business in California must notify their California customers if they discover or suspect that nonencrypted data has been accessed without authorization. This applies even if the business is not located in California, as long as you have customers there, and no exception is made for small businesses.

9 Community Broadband Act of 2007

This is a piece of pending federal legislation that was introduced in July of 2007 as U.S. Senate Bill 1853. In April 2008, it was placed on the Senate Legislative Calendar under General Orders and is still winding its way through the legislative process. This federal law would prohibit state and local governments (municipalities and counties) from passing laws that prohibit public telecommunications providers from offering Internet services.

This is in response to laws passed in a few states, as a result of lobbying from the telecom industry, that prohibit cities from installing and operating public broadband networks, such as public wi-fi networks. The big telecom companies have a vested interest in preventing cities from establishing networks that could compete with their own services by providing free or low cost Internet services because the public services are partially or wholly taxpayer-subsidized.

If this law passes, it could make it easier to find free or low cost ISP services in cities that choose to build public networks. On the other hand, it could (depending on how it's funded) cause tax increases for those who live in those municipalities, including those who don't use the public networks.

10 Pro IP Act

Back on the copyright front, the House of Representative recently approved by an overwhelming majority HR 4279, which imposes stricter penalties for copyright infringement. It creates a new position of "copyright enforcement czar" in the federal bureaucracy and gives law enforcement agents the right to seize property from copyright infringers.

This may all sound fine in theory, but when you look at the way other seizure and forfeiture laws have been applied (for instance, the ability of drug enforcement officers to seize houses, computers, cars, cash, and just about everything else that belongs to someone tagged as a suspected drug dealer --, and in some cases not returning the property even when the person is acquitted or not prosecuted), it makes many people wary. Read more about the bill at http://arstechnica.com/news.ars/post/20080508-house-overwhelmingly-passes-controversial-pro-ip-act.html.

Some local jurisdictions have already established seizure authority for piracy. See http://arstechnica.com/news.ars/post/20080509-piracy-now-public-nuisance-in-los-angeles-county.html for more information.

Additional resources

- TechRepublic's Downloads RSS Feed XML
- Sign up for the Downloads at TechRepublic newsletter
- Sign up for our IT Leadership Newsletter
- Check out all of TechRepublic's free newsletters

Version history

Version: 1.0
Published: May 16, 2008

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to drop us a line and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Content Team