Is that a Felony on Your Computer?

Rick Hellewell, security@digitalchoke.com
October 18, 2003

There are several federal laws you need to worry about if you are into network security, administering a network, or even if you are doing a bit of network "surfing". This report is my current knowledge on this subject. You'll need to know that I am not a lawyer. This is just information I have gathered, and my analysis of that information. It's based on a presentation from Mr. Richard Salgado, a US Department of Justice Lawyer that was given at the SANS Security Conference in San Diego CA in March 2003. (A PDF file of his presentation from the 2002 SANS conference is at http://www.sans.org/SANS2002/1-9_Salgado.pdf.). I've also done some other research about this over the past year.

If you use a computer, if you are a network guy, or even as someone just on a network, you should be aware of a few things that can get you a new place of residence with doors and walls of steel.

Let's start with a couple of concepts. When I discuss a 'network', that can be a network at work, or just your home connection to the Internet. A "provider" is someone that gives you access to the network. A provider could be your Internet provider (they give you access to their network, which gets you access to the Internet network). It could also be your company, who give you access to the company's network. Or it could be you with your home network. These concepts are important to keep in mind as you wander through this discussion.

This discussion is about scanning or auditing the network, or even 'sniffing' (sort of electronic eavesdropping) information that is on the network. And it also applies to looking at files on the network, or configuration settings, or email messages. In this discussion, we'll usually use the term 'network monitoring' for the various types of monitoring, scanning, or auditing.

There are lots of software tools that are available for looking around a network. This discussion won't talk about specific tools, just the fact that there are ways that one can look into data on the network, or traveling through the network. These tools let you look inside files, network traffic, mail messages, or server settings. It's this looking that can possibly get you in trouble.

But before we get to why that "just looking" can be a problem, let's look at a couple of federal laws.

There are three main US (federal) laws that pertain to network monitoring: the "Wiretap Act', Pen Register Statute, and the Electronic Communications Privacy act. All of these laws affect any monitoring of the network, such as packet sniffing, email message monitoring or analysis, looking at files on the network or on a workstation, monitoring access to the Internet, etc.

The Wiretap Act prohibits the interception or monitoring of any wire communications, including phone calls and electronic sniffers. There are allowable exceptions:

- If you are the 'provider' (the owner of the network)
- To monitor a 'computer trespasser' (someone who is intruding on your – the provider's – network
- If the user consents to the monitoring
- Interceptions because of a court order
- Extension telephone connection (doesn't really apply here)

- Inadvertently obtained criminal evidence (such as a technician working on a workstation and during the normal process of repair discovers illegal material)
- If the information is accessible to the public.

This means that **any** monitoring of any network traffic might be a violation of the Wiretap Act *if you don't carefully put in place exceptions that allow the monitoring of the network*. (More about that in a bit.) Remember that monitoring of the network can include:

- Intrusion detection software that inspects network traffic
- Network scanning of any type (port scanners, vulnerability scanners)
- Mail scanning or filtering (looking at the contents of a message for spam-filtering or illegal or objectionable material)
- Web filtering (looking at what sites or Internet content people are accessing to prevent access to any site)
- Remote control (or viewing) of a computer (electronic 'shoulder-surfing', where you can see what another user is doing on their computer)
- Key logging software (capturing keystrokes and/or screen images)
- Looking at other's network or workstation files (just reading files on the network)
- Any forensic analysis of data on a network or workstation (such as data stored on a hard disk, or data that is captured with a network sniffer)
- Probably just about anything that affects any file or data or content or process that is not your own personally created information

The Wiretap Act allows you (if you are a Provider) to do reasonable monitoring of the network to protect the Provider's rights or properties, or if the activity is a necessary part of providing the service of your network. Only the Provider can exercise this right; law enforcement cannot (except with proper legal authorization like a court order). The provider can give legally accessed information to a law enforcement agency voluntarily, but law enforcement cannot do the monitoring. This exception (the 'reasonable monitoring') allows a technician to work on data (a workstations' hard disk, or a data from a network sniffer) as part of a troubleshooting/repair process, but you have to be careful about the 'depth' of what you look at.

The Wiretap Act lets a Provider track the actions of a hacker/intruder to prevent damage to the Provider's network. But it can be a problem if you let it this tracking goes too far (page6).

If the user consents to monitoring, the Wiretap act allows such monitoring. *This is a very important point. Without a user's consent, your actions – any monitoring – may be a violation of the Wiretap Act.* And that violation of the Wiretap Act is a felony, by the way. The penalty is up to 10 years in a federal prison (and probably not one of those 'country-club' places).

There are several types of user consents that you should have enabled on your network. **All** of these consents are important, and they can work together to allow you to comply with the "consent exemption' of the Wiretap Act.

- Banner the network: show a banner message every time a user accesses your network. The message should be simple, and alert the user that
    - Network monitoring is in place

  - There is no expectation of privacy
  - Continued use of the network is consent to this monitoring
  - Make sure you don't use a word like "Welcome", as that implies letting the user do anything they want

- Obtain the written consent of the user. This consent form should include the above information, acceptable use guidelines, etc. It should be signed as a condition of accessing the network.
- Any other consent agreements, such as employment agreements, business policies and guidelines, etc., add weight to the user's consent to monitoring. The more consent, the better.

It is important to note that the user needs to actively consent to network monitoring. (And repeatedly getting that consent couldn't hurt.) This can be done with a sign-on message that includes a "Yes" button that the user must click on before they get into the network. You could include it as part of the login process.

The provisions for active consent were a bit weak in the case of a hacker's access to your system. So the Patriot Act added additional weight to the 'hacker consent'. This consent allows law enforcement to monitor the activities (but not necessarily the content, unless under court order) of the hacker. It does not necessarily allow the Provider to monitor. But the other consent agreements are a very good protection for the Provider's monitoring of the network and content.

The Pen/Trap Act allows for monitoring of email messages, but that allowed monitoring only applies to the message header (envelope) information, not the contents of the email message. Looking at or monitoring the contents of email messages (such as email filtering or anti-spam programs) is on example of actions covered by the Wiretap Act. The US Patriot Act amended the definition of 'pen register' to allow the monitoring of electronic/data communication.

The Pen/Trap Statute allows Provider to use pen/trap devices (such as sniffers, email or web monitoring software) to protect the Provider's network against abuse or unlawful use of the network. But, **you must have the consent of the users** of your network, or a lawful court order to allow legal use of pen/trap devices on your network.

The Patriot Act, and the Homeland Security Act, allows any communication that passes through a Provider's system to be monitored (again, usually with the user's consent), even if the information passes through several jurisdictions. So if you live in Oregon, and your information goes through servers in Colorado or New York., the information can be monitored, and a legal court order doesn't have to be obtained for every court jurisdiction that the data passes through.

Disclosing any information gathered through monitoring the network has to abide by the Electronic Communications Privacy Act. Information covered by this act includes stored information (files, email messages), log files, personal information (user name details), IP Address, etc. The ECPA says it is illegal (without authorization) access a file on a users computer or network drive, or prevent a user from accessing their information (such as email messages they haven't read yet). The example from Mr. Salgado's presentation says:

> For example, a system administrator, who, outside of regular duties and otherwise without permission, copied one or me unread messages waiting in another employee's email in-box, is in violation of this law.

The penalties for violating terms of the ECPA were increased as part of the Homeland Security Act to be one to five years, up to 5-10 years. Mr. Salgado stated that these two laws are quite complex.

An important fact is that it is unlawful to access information on the network when it is done outside your normal or regular duties. Just because you can install a network sniffer on your computer, that doesn't allow you to legally capture information on the network. (Remember that the 'network' can also be the Internet.) A system administrator (or even just a 'user') who, outside of their regular duties and otherwise without permission, who copied one or more unread messages waiting in another person's email in-box, is in violation of these laws. Just because you can do it, doesn't mean that you have the legal authority to do it.

Here's an example. You are at home surfing the Internet, and you come across a tool that allows you to 'test' a remote server's security. It looks sort of interesting, so you decide to give it a try. You set it up to scan a bunch of IP addresses, and watch it work. Bam! You may have just committed a felony.

Or you decide to use a similar tool to test server passwords on your company's network. Even though you are not the network guy, you have a bit of computer geek in you that wants to give it a try. So you try a password hacking program against a server on your network. Bam! You may have just committed a felony.

These are not 'schoolbook examples'. There are actual instances of this type of actions. And there are some people in prison because of these seemingly benign activities. Remember that the penalty for violation of these federal laws is up to 5 years in a federal prison and up to 10 years for a repeat offender.

So, how do you protect yourself if it is your job to keep track of the network? Or if the boss tells you to look at an employee's email or computer files because they are suspected of passing information to a competitor? Of if you need to monitor the network to make sure there aren't any network bottlenecks? Or you need to scan all email for objectionable or illegal content (anti-spam filtering)? Or if you need to limit user's access to offensive (adult or otherwise) web sites in order to protect your company against sexual harassment actions?

All of these things are typical actions for a network administrator (or an Information Security guy).

According to my research, this is what you need to do to protect yourself or your company if your job is to monitor or do technical support your network.

- Make sure that you have the consent of the users to monitor the network. You can do this with login banners, acceptable use policies that the user signs, employment agreements, etc. The more consent you get, the more you are protected. Make sure that vendors who have access to your system also sign agreements. (And non-disclosure

agreements for vendors and employees are good things.) Issue written policies and guideline to your users, such as Acceptable Use policies (note that “policies” seems to be a stronger word than “guidelines”).

- Make sure the users know that monitoring may take place at any time, and there is no expectation of privacy when using your network
- Make sure that your monitoring has a business purpose, not just because you are curious.
- I have a “Get Out of Jail Free” file that contains memos and notes and authorizations for my access and monitoring of the network. You might want to keep a copy of that stuff off-site, but be careful about securing any confidential information.
- Make sure that you have the legal guys in your company review policies and procedures for compliance with laws.
- If a law enforcement agency shows you a court order to get information, get your legal department involved immediately.

Consent is very important if you are to legally monitor your network. And you should make sure that it is your job to do that monitoring. If it is not your job, or if you decide to do a little hacking on your own, be very careful. The US federal laws are very enforceable. There are people in federal prisons that can attest to that.

So, be careful out there. Make sure that there isn’t a felony in your computer.

Additional Resources

There are lots of web sites that you might want to look at to get more information. Here are the ones that I have found useful. It’s not an in-depth list, but there are lots of links to other resources on these sites.

www.sans.org - contains many security-related articles, research papers, sample policies, and a good mailing list of security-related news. They also have excellent training sessions worldwide, and some good tools to analyze the security of your system. Many links to other sites are http://www.sans.org/resources/popular.php.

www.cybercrime.org - the “Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. Department of Justice”. It contains many links to related sites.

http://www.nipc.gov/index.html - US Department of Homeland Security. It has a section on “Legal Issues” , and publications.

http://www.issa.org/ The Information Systems Security Association, with monthly artcles on security issues, and information on local chapters that may be in your area.