Countermeasures

---
by Thomas Icom

"An ounce of prevention is worth a pound of cure." - Ben Franklin

With the recent crackdown on "computer hackers" and evidence that more busts are on the way modem users in general have been quite concerned that by exercising their rights they could have the S.S. knocking on their door because they called a BB S. This has prompted many telecomputists and computer bulletin board systems to cease operations for fear of being raided.

With the recent raids at Steve Jackson Games and Jolnet perhaps these fears are reasonable. However, if you are committing no wrongdoings you still, despite the KGB and Gestapo like actions of the Secret Service have the right to exercise your freedom of information access via electronic media. There are only three laws relating to the use of modems and BBS systems. The first two are toll fraud and computer trespass. Toll Fraud is the avoidance of paying telephone company service charges. Computer trespass is the unauthorized access of a computer system. When you call a public BBS, or a private one you are a member of and pay for the call you are not committing either of these crimes. While they may not like the fact that you have a computer and modem, they can't touch you. The other law is not particularly computer related and goes under many different statues, but in all cases deals with encouraging people to commit illegal acts. This law applies to "illegal" information on BBS systems.

What is "illegal information"? Well any information which has no educational or informational purpose that encourages people to commit a crime. When applied to BBS systems it only includes calling card/long distance telephone service codes, credit cards, and computer passwords /login sequences. That's all. Hacking and phreaking information has an educational purpose in that it teaches people computer security, and shows dangerous flaws in systems that could be used by someone for nefarious purposes. As long as no direct encouragement is given to exploit these flaws the information is not illegal and is thus protected by the First Amendment: freedom of speech. If you are a BBS owner you can have all the hacking and phreaking g-files and message bases on your system and they can't do a thing.

If they do, they open themselves up to a law suit. The prime examples of this are the Private Sector, OSUNY, and The Central Office BBSes. Private Sector was raided, but no charges were filed because there were no codes, passwords, or credit cards on the BBS. OSUNY and Central Office were online for years and were the subject of many investigations, but no action was ever put forth against these BBSes as n o illegal information was on them. The precedent is there. In order to evoke First Amendment protection on

your BBS or newsletter display a clear statement that the information is for educational purposes only, and that no illegal use is implied or suggested.

Now of course the Secret Service often violates these laws despite the fact that in doing so they don't have a legal leg to stand on. They do this on the basis of a technique which has been used from the Middle Ages, down through Nazi Germany, up to the various activities of the KGB in the Soviet Union: Fear and Ignorance. People who are ignorant of the law become afraid because in being unaware of their rights they don't know what the government can and more importantly can't do. Due to fear and ignorance they can operate carte blanche because they know the chance of reprisal by some irate citizen is very low. Also, once they raid someone they can gain intelligence on other modem users/"hackers". Once they have the info on the system, they can give it back. They accomplished what they set out to do.

Fortunately you can fight back, and your efforts will eventually be rewarded. On many of the busts the S.S. has gotten burned, and it has been plainly shown to them that they can't continue to operate this way. However no modem user has yet had the balls to sue those bastards. With the current state of affairs the charges get dropped due to various improper procedures, but no specific precedent has been set to make them liable for their illegal activities. Once they lose in a lawsuit brought against them by a modem user they screwed over, we'll see some severe restructuring in that particular branch of the Treasury Department.

The first stage in protecting yourself is to be aware of the laws and your rights. Knowledge is power, and they are well aware of that. In light of that they watch themselves when dealing with people who know their rights because they know t hat those people will have them nailed to a wall if they slip. Know your rights and be adamant about them.

The second stage is that if you deal in anything even slightly controversial take precautions to secure the info in your system. Encryption is a definite must, as well as any other tricks to hide data on your system and prevent tampering. When encrypting data stay away from DES. While everyone say it's the best system the NSA has not recertified it, and the fact that it was developed for the government leads enough credence to the possibility of there being a back-door in the algorithm. About the best personal encryption system I've seen out there is the Absolute Computer Security System scheme by Consumertronics. A good idea is to double encrypt the data with two different algorithms. From what was shown by the recent busts in Operation SunDevil the technological expertise of the agents wasn't too high. To quote Lloyd Blankenship of Steve Jackson games, "They don't know what subdirectories are." This means that any moderately sophisticated data hiding technique should stump t hem. I would expect though they should be getting better as time goes on. What I would do is use some of the tricks that computer viruses use when hiding data. Marking off used or "bad" sectors to put your data on, or appending it to ordinary

programs. One of the best things you an do is put your data on floppy disks, then store them in a container containing a large electromagnet hooked up a tamper switch. This way if they raid you just give the box a good push an d everything's wiped. For paper documents use a burn box. This is a sturdy metal container with an incendiary mixture hooked up to a tamper switch. When they mess with it, everything is turned to ashes. You can store data "off-site" where their search warrant doesn't cover . This can be as simple as burying it in the backyard/under the shed or in a "friend's" house. Rig up special hidden access programs to your system, preferably in ROM, so that if your data isn't accessed in a certain way it gets wiped.

If you want to be real nasty, put some fake "incriminating" data on your system for them to bite onto. Good suggestions would be random phone numbers with an extra 4 digits attached or random 16 digit numbers with fake names. This way it looks like they've found calling cards or credit cards. Then if they are stupid enough to take you to court, you can explain where you got them from.

Even if they aren't stupid enough to fall for that trick, you still have wasted their time. Another idea would be to make a fake database of fellow hackers. This way they waste time tracking down all those false leads. These techniques would serve to make fools of these assholes.

Now if you do happen to get raided or put under surveillance there are a number of things you can do. If you see any "strange activity" outside your house call the police. If some "strange people" come on your property you can warn them that it's private property and then have them arrested for trespassing. You can also go outside and start taking pictures or videotaping them. That pisses them off but they are generally loath to do anything because you'll have evidence against them. If they come over to ask you questions politely refuse and tell them to talk to your lawyer. If they persist have them arrested for trespassing and harassment. You should also check their ID. John Williams and I have often run into corporate and idependent goons who decide to visit you in some sort of attempt to intimidate you. If their ID looks fake or it's otherwise obvious that they're not real law enforcement then have all the fun you want with them! If you receive a phone call, turn o n your tape recorder, refuse to answer any questions, an give them the name and number of your lawyer. The tape recorder is important as you'll want evidence of the phone call if their manner of talking to you on the phone opens them up to legal repercussions. And always before you pick up, state the date and time on the tape, and make sure they identify themselves to you.

If government agents come with a warrant call your lawyer, and document everything. Actions they commit on the search warrant may screw them later, but you'll need evidence. Videotape them if it's feasible, and if you have a friend in the press call him/her. Above all invoke your right to remain

silent, and don't help them by opening your mouth. With the recent rash of Gestapo-style no-knock warrants a modem using friend of mine has started keeping a .44 Magnum by the door. His explanation is since he's not doing anything illegal if someone comes crashing through the door he's going to assume its a burglar or psychotic and protect his property and family until the police come. We of course don't recommend that you follow his example, but the choice is yours. After all a law abiding citizen has the right to defend himself.

After the bust have your lawyer keep on them like a fly to manure. According to the law a search warrant is supposed to be for gathering evidence for an indictment. If no indictment is forthcoming (none should be if you're clean) then demand your property be returned to you. In any event you should always file suit and seek legal charges against them. Just the simple act of doing that creates hassles for them.

Before I wrap this up, let me state that I have nothing against law enforcement people. Most of the police officers out there do a fine job, and are good people. However, the few rotten apples in this country's law enforcement infrastructure do a lot to blacken the name of police officers everywhere. I am also amazed that with all the murderers, rapists, and child molesters running around lose in this country, our police agencies are so quick to jump to the whim of some whining, clueless , control-addicted corporate bureaucrat; who's probably broken more laws than the worst hacker ever could, and go after innocent telecomputists. (Why wasn't Neal Bush arrested?) I would tend to believe that child molesters should have a higher hunt-down priority then kids with computers; however sometimes that doesn't seem to be the case.

Driving Tips

Motor vehicles are probably the most common form of transportation used today. Perhaps this is why most people involved in an operation get busted while driving. In New York & many other states, your rights are nonexistent while you're behind the wheel, and you can get pulled over and searched for any reason. So, to stay out of trouble and avoid any problems that might result in getting pulled over, I've put together some guidelines that should help keep you out of trouble while you're on the road.

1. Keep tabs on the local law enforcement agencies. While most cops are more or less decent and won't bother you as long as your not driving recklessly, there are a few bad apples who will bother you for whatever reason. Also, remember that you have no rights on the road. You're fair game for any reason. Get ahold of a mobile scanner and hide it behind your dashboard or in a seat. Scanners are illegal to have in vehicles in some states and much frowned upon in others. Run a remote speaker to a convenient but hidden spot with a hidden switch to turn it off. This way they can't see anything that looks suspicious, and you can cut out the audio quick if you get stopped. Also remember to program in secondary car-

to-car and mobile to base frequencies. This will give you an indication of law enforcement activity nearby you and allow you to take appropriate action should your plates get checked all of the sudden.

2. Drive at the proper speed. By that I mean not too fast and not too slow. Not only can you get pulled over for speeding, but if you drive too slow, you'll get pulled over for being suspicious.

3. Know your geography. Intimate knowledge of the roads in your area of operations is essential. This way, you can take alternate routes if there is an obstruction down the road as well as know what roads not to take so you don't make an evasive turn into a dead-end street.

4. Stay off well-traveled roads whenever possible. You're less likely to get stopped on a secondary road.

5. Drive something appropriate looking for your locale. If you drive something too fancy or too beat-up you will attract more attention to yourself.

6. Keep anything attention getting out of sight. If you get stopped, and nothing is visible, then there is less cause for them to search your vehicle.

7. Obey all the traffic laws. This is common sense, but many people who were wanted criminals got nailed by a simple traffic infraction stop.

8. If you get pulled over, be polite even you are insulted and harassed.

Also, don't make any sudden moves. Again, common sense, but some stupid people think that they have to mouth-off when they get pulled over and given a hard time. They're the ones who usually get busted.