The PARANOID Newsletter

Because they ARE out to get you.

Introduction

This is the first issue of the PARANOID newsletter. This newsletter is for the person who takes their privacy VERY seriously. Lets face it, America is a POLICE STATE. Anything the government doesn't like is now considered terrorism. What would our founding father say if they were alive today! How is the government eroding your rights you ask? Through Terrorism and Sex offender scares of course! Today's politicians can pass all kinds of laws that destroy Americans freedom because the average citizen is lazy and stupid.

Don't expect the constitution to save you, its worthless paper. If the constitution was worth the paper it was printed on there wouldn't be warrant less searches and wiretaps, foreigners wouldn't be TORTURED and the FBI wouldn't have the authority to perform Sneak and Peek searches. You do know what a sneak and peek warrant is don't you? Have you ever heard of a National Security Letter?

Sneak and peek search warrant: A search warrant authorizing law enforcement officers to secretly break and enter into a persons home or business without the owner's or the occupant's permission or knowledge and to clandestinely search the premises. Any crime including misdemeanors may be used to justify a sneak and peek warrant.

National Security Letter: A warrant like document invented as a method of circumventing the Right to Financial Privacy Act in 1978. The Patriot Act permits these NSL's to be issued without consulting a judge, merely a Law Enforcement Supervisor. It is frequently used to obtain private records of Americans' Internet service providers, financial institutions and telephone companies. NSL's contain a gag order that prevents the recipient from consulting a lawyer or notifying the target of the investigation.

NOTE: An internal FBI audit found that the bureau violated the rules more than 1000 times in an audit of 10% of its national investigations between 2002 and 2007. Over 20 of these involved requests by agents for information that US law did not permit them to have.

In fact the FCC, the government department that licenses manufactures of radio products CLAIMS to have the authority to inspect your home without a warrant and ANYTIME. If you have a cellphone, CB radio, or anything else that uses radio waves, the FCC claims it can enter your home at any time to inspect it. Donald Winton, the operator of a CB rebroadcasting an AM radio station, refused to let an FCC official in his house, but did turn off the radio. Winton was fined $7000 for refusing the FCC official entry into his home. Remember, the FCC official is not a police officer. The fine was reduced to $225 after he proved he had little income. Fortunately, the best the FCC can do is give you a fine.

This newsletter will teach **YOU** how to protect

Your home and office from illegal searches.
Your gun ownership rights.
Your financial records.
Your home, vehicles, cash, etc.
How to have wiretap proof communications.

Learn how the government is recording your every move and how to stop it!

The first order of business is to “get your mind right”. Take all your thoughts of legal protection, fair play, honesty, good faith, cooperation and throw them right out the window. Now lets start clean with a new set of assumptions about the government.

The government wants to do the following:

Control everyone and everything on the Internet.
Take away the savings of the entire nation through inflation.
Pump propaganda into your home through biased journalism.
Scare the entire American population into signing away their rights.
Permit a MASSIVE inflow of Latino Illegal Immigrants into the US.
Brainwash and dumb down children in public school and deter homeschooling.
Take control of healthcare decisions and private medical records in the United States.
Record every number you dial and monitor every step you take by tracking the E911 GPS in your cell.
Monitor financial transactions through credit card records, bank records, Currency Transaction Reports, etc.
Register, ban and ultimately confiscate all privately owned firearms, at least any firearm good for self defense.

Basic tactics to combat the FBI

Safeguard your rights to own a firearm:

IMPLEMENT THESE STEPS IMMEDIATELY BEFORE FIRARMS ARE BANNED

Buy several high powered firearms and bury them in watertight containers in the ground.

Use the gunshow loophole to buy firearms from individuals directly, hassle free.

Buy a substantial amount of ammunition, especially hollow point and specialty ammunition.

Buy high capacity magazines.

Buy mail order black powder firearms hassle free.

Don't have gun products sent to your home address.

Don't be associated or affiliated with any gun ownership organizations.

Don't keep more than one or two guns in your home, keep the cashed away incase the government seizes or bans them.

Use Pelican brand waterproof cases to ensure your guns are safe underground. (Wrap the case in heavy duty trash bags to keep the case clean)

Don't let ANYONE know about your extra firearms or that you are interested in firearms.

Buy Shotgun News magazine to get good deals and hard to find items.

Safeguard your computer:

DO NOT USE MICROSOFT PRODUCTS

Use whole disk encryption such as Truecrypt or PGP encrypt everything on your PC with a strong password.

Strong passwords are completely random, 45 characters or larger, use upper and lower case and symbols.

Never write down your password. Perhaps burying it in an underground container would be acceptable.
Use software that over writes the unused portion of your hard drive with random information.

Overwriting data makes it impossible to recover forensically, be use to use the 7 pass DOD approved method.

Use the Apple operating system, OS X. Windows is so insecure it must be replaced entirely.

If you must use Windows, use it as a decoy computer which the government can steal and think they got your PC.

Buy hardware encryption from Addonics.com, buslink.com or similar hardware encryption products.

Always use a second layer of software encryption such as PGP or that uses passwords since your 5th amendment right will prevent you from being forced to divulge a password. A physical key can be subpoenaed.

Keep confidential information on an encrypted laptop, try to lock it in a hidden safe.

Never leave a running cryptographic system unattended. If the government raids you, they can look at everything.

Always check to make sure there isn't a hidden key stroke recorder plugged into your keyboard.

Communicate securely with bitwiseim.com's encrypted instant messenger. The program allows secure voice conversations, secure IM's, secure file transfers and more! The encryption must be done on your end, never rely on the service provider to encrypt for you like Skype. YOUR ACTIVITY CANNOT BE WIRETAPPED, NOT EVEN BY THE GPVERNMENT WHILE USING BITWISE – IT IS ALL ENCRYPTED.

Use encrypted offshore proxy servers to establish a SSL encrypted link or other encrypted tunnel to use the Internet. To your Internet Service Provider it looks like your only talking to one server in a foreign country and are just speaking gibberish. YOUR INTERNET ACTIVITY IS NOT PRIVATE AND CAN BE WIRETAPPED. Encryption is your ONLY protection against wiretapping and it cannot be broken by the government. Neomailbox.net is a good start.

Consider storing all confidential data in encrypted form on a wireless hard disk that is physically hidden in the walls of your house and using an X10 controller to turn the device on and off. The PC can boot from a small hard disk or DVD linux boot image and then connect to the wireless hard disk. USB wireless hubs can be very useful.

128 bit and especially 256 bit and larger key sizes of encryption are UNBREAKABLE if you use RANDOM 45

character passwords or longer. Always use a known safe encryption algorithm such as AES, Triple DES, Twofish, Serpent or Blowfish. Never give anyone your password. Rely on the 5th amendment to not give it up.

When using strong encryption you must use high security tamper proof seals on ALL your equipment. Polylabel.com has serialized holographic tamper proof seals that are EXCELLENT. If your computer can be tampered with, the next time you type in your password the "bug" will record it and then the KGB can break your encryption. You have to be dumb enough to type the password in after the tampering has occurred.

Always smash and burn a hard disk, CD or other computerized media when discarding it.

Always erase and overwrite or otherwise destroy obsolete or unnecessary copies of confidential information.

Always update your computer with security patches. (Windows update, Apple Update)

Safeguard your home against illegal searches:

Buy high security anti bump locks such as the commercial Medeco lock for the front and back door. Do not use a home version. Medeco keys are harder to duplicate and are extremely lock pick resistant. Pin all your windows.

Scan all paper records that must be kept and store them in an encrypted computer that does NOT connect to the Internet. Burn or shred the originals.

Use a metal container to burn confidential material in, such as a metal wastebasket. If you have a fireplace, place the container inside when burning. If you choose to use a shredder use at least a crosscut shredder, a micro cut is better still. Always stir the ashes when burning paper, adding water makes the ashes disintegrate.

Hide confidential items inside home made hiding spots. A junk VCR bought from the thrift store can become an excellent place to hide your goodies. Put it with your other stereo equipment and no one will suspect a thing. If your tech savvy, build a small computer like the mac mini into the VCR case and its a disguised PC! Just use wireless keyboard and mouse and a HDTV for the monitor. Add "void" tamper seals to complete the disguise.

Be careful about having controversial material at home where it could be found by the government. Pornography, racist literature, gun magazines, unpopular religious material, and all sorts of legal but controversial material should be WELL hidden. Get the book "How to hide anything" by Michael Connor

> With little effort and expense, you can hide cash, armaments and even family from the menacing eyes of burglars, terrorists or anyone. Learn how to construct dozens of hiding places right in your house and yard. Here are small hiding places for concealing money and jewelry and large places for securing survival supplies or persons. More than 100 drawings show how to turn ordinary items into extraordinary hiding places.

Also read "How to be invisible" by J.J. Luna and visit his website with discussion forum at howtobeinvisible.com.

Learn to use Pelican cases to hide important things in the back yard underground. They are 1000x safer under a little dirt in the backyard rather than being in the house for the government to find.

Safeguard your money:

Invest in gold, silver, platinum and palladium bullion, bullion can be redeemed anywhere for local currency and inflation will never eat away at the price of precious metals. Bulliondirect.com is an excellent place to buy.

Hold most of our cash out side of a bank. Keep your cash and bullion safe and hidden away, rather than keeping all your money in a bank where it can be seized by the IRS, creditors or the government.

Do not use credit cards or write checks! They show how much money you spend, where you spend it and credit cards in particular can give detailed accounts of the things you buy. NEVER USE CREDIT CARDS!

If someone opened up a bank account, say a corporate bank account and kept your name off of the records. You could use ATM cards to withdraw cash and to deposit money into the bank. By using ATM's you can conduct virtually all your banking with a machine instead of a person who would ask for ID.

Prepaid debit cards can be used to make telephone and online purchases safely.

Prepaid cellular phones can be used to prevent invasions of your privacy and can be discarded in an instant.

Use money orders rather than checks when possible. Some organizations like stock brokers don't like getting money orders too often. Throw in some cashiers checks, regular checks from “friendly bank accounts” and other varying payment methods to prevent looking like a drug dealer / money launderer.

Cash checks at a liquor store, be careful that the bank has no real address for you, the government will be able to get whatever information you supply them.

Never move money in any amount that would trigger a Currency Transaction Report. Stay well under $10,000 when doing business whenever possible, it sets off reports to the IRS.

Set up LLC's to own things for you. The book “How to be invisible” by J.J. Luna explains the very easy process. Your company can own houses, cars, planes, just about anything imaginable. When a police man runs the tags on your car he'll will see your information. When they run the tags on a company car they see nothing but the company as the owner. YOUR TAGS WILL BE INVISIBLE. This can easily be done on just about anything, including utility bills which can be used to track you.

Always keep a little checking account open with a small amount of money in it. It is a thermometer to see if anyone tries to seize your assets. You will be put on notice and it'll only cost you a mere $30 deposit.

Don't fall into debt slavery.

Do anything you can to prevent giving out a social security number, its the standard way to track you down.

If you can work for cash, can be self employed or work out some other friendly arrangement, do it.

Do everything possible to reduce your taxes, the government uses your tax money to do evil. Mail order / imported cigarettes, rolling your own cigarettes, brewing your own beer / wine prevents the government from getting tax revenue.

Social security is a fraudulent Ponzi scheme, do everything you can to avoid it.

Make a “bug out bag”, a backpack with bottled water, canned food, survival knife, money, matches, clean set of sturdy clothes, etc. designed to hold you for 72 hrs in the event of a disaster. ALWAYS have this bag ready.

Learn about food storage from the Mormons, every member has a years supply of food just in case.

Safeguard your privacy:

Set up a front to receive mail. Use commercial mail boxes, remailers, po boxes, “front locations” and other tricks explained in how to be invisible to act as your official address. Consider paying an RV grounds to receive your mail and act as a home address when your “on the road”. Think “room for rent” for a “front” address.

Never let your true name be associated with your true address. Don't even order pizza with your true name.

Want to start fresh? Move to a new state, change your name in that state and then move again. Don't bother changing your drivers license until your in the final state. Also consider that Arizona has drivers licenses that only expire on your 65 birthday!

Random tip: Need to visit a doctor confidentially? Visit a doctor and pay cash, use a fake name and give false information for everything. Noe of the information is necessary if your paying cash, especially the social security number. Cash patients don't need that bit of information. Get checked out and never give out your true identity. Filling a prescription is also completely hassle free, WORST CASE if you have trouble, mail order the prescription next day or two day. You can also ask the doctor for free samples of the medicine you need.

What to do if the police want to talk to you

"GOOD MORNING! My name is Investigator Holmes. Do you mind answering a few simple questions?" If you go to your door one day and are greeted with these words, STOP AND THINK! Whether it is the local Police or the F.B.I. at your door, you have certain legal rights of which you ought to be aware before you proceed any further.

In the first place, when the law enforcement authorities come to see you, there are NO "simple questions". Unless they are investigating a traffic accident, you can be sure that they want information about somebody. And that somebody may be you!

Rule number one to remember when confronted by the authorities is that there is NO law requiring you to talk to the Police, the F.B.I., or a representative of any other investigative agency. Even the simplest questions may be loaded and the seemingly harmless bits of information which you volunteer may later become vital links in a chain of circumstantial evidence against you or a friend.

DO NOT INVITE THE INVESTIGATOR INTO YOUR HOME!

Such an invitation not only gives him the opportunity to look around for clues to your lifestyle, friends, reading material, etc; but also tends to prolong the conversation. And the longer the conversation, the more chance there is for a skilled Investigator to find out what he wants to know. Never open your door to an Officer. They can shove their way in. Don't open your door with the chain-lock on, either. Police are known to kick in doors. I should add, that when you let a Police Officer into your house, then he is automatically authorized to do a weapons search (supposedly for his own protection) and this can lead to all kinds of problems!

Many times a Police Officer will ask you to accompany him to the Police Station to answer a few questions. Often, the authorities simply want to photograph a person for identification purposes, a procedure which is easily accomplished by placing him in a private room with a two-way mirror, asking him a few simple questions, and then releasing him. NEVER agree to go to the Police Station. Simply say, "I have nothing to say."

If the Investigator becomes angry at your failure to cooperate and threatens you with arrest ... STAND FIRM. He can't legally place you under arrest or enter your home without a warrant signed by a Judge. (There are exceptions to this however, as in instances where he has witnessed you commit a crime, and there are times, too, where he can enter without showing a warrant up front, known as a 'no knock' entry.) However, if he indicates that he has such a warrant, ask to see it. We've heard of Cops waving a piece of paper around, claiming it was a warrant. A person under arrest or located on the premises to be searched, generally must be shown a warrant if he requests it, and must be given a chance to read it.

Without a warrant, an Officer depends solely upon your helpfulness to obtain the information he wants. So, unless you are quite sure of yourself, don't be helpful. (Note: Don't fool yourself into thinking you can talk or lie your way out of the situation. Don't be smug and think, "All Cops are stupid" and you can pull a 'fast one.' Most Police are smart individuals, they're good at what they do, and the only thing you will do is talk yourself into jail.)

Remember, talk is cheap! But when it involves law enforcement authorities, it may cost you, or someone close to you, dearly. Remember the 5 words -- "I HAVE NOTHING TO SAY." It has worked for us many, MANY times. And it will work for you! There is never, ever, a situation where talking to the police can HELP you. In court any favorable statement to law enforcement is considered hearsay and is inadmissible.

Security seals offer serious security.

Have you ever tried to open up a computer system with a warranty sticker sealing the removable cover to the frame? As soon as you opened the computer case the warranty seal separated with the repeating text “VOID VOID VOID”. Considering the impracticality of brute forcing strongly encrypted files, anyone serious about getting your files will look for another way; hardware tampering is the easiest and most common way to defeat password based encryption systems and capture text. Think of file encryption as a vault door, if you want any real security you have to prevent anyone from breaking in through a glass window.

Holographic Security Seals deter anyone from opening your equipment and alert you if your equipment has been tampered with internally. If your equipment is compromised an attacker could install hardware without your knowledge that is designed to capture your keyboard text or some other input or output that has been decrypted, thereby bypassing the encryption.

The best seals have serial numbers. Some are translucent and others are opaque. We recommend using more than one type security seal so it would be harder for an attacker to counterfeit, lift, cut, chemically dissolve the binding glues or otherwise attack the seal. Seals cost the attacker time and usually hardware tampering is done secretly on site. Every extra minute spent in your office increases the risk of discovery to your attacker. While some may consider this to be excessive security, the cost of seals are only a few dollars. If your serious about having secure equipment they are a requirement. The only real world way to beat strong encryption is to cheat and install key stroke recording devices or otherwise tamper with the systems hardware.

Security seals on computer equipment are rather uncommon and will completely surprise your would be

spy; I would be very surprised to hear of an attack where the spy brought chemical solvents and lifted multiple seals on the first entry. I expect the number one attack on seals to be thin razor cuts. If you aren't careful in your examination you can easily miss a fine razor cut exactly along the seam of the equipment, other attacks are simply failure prone or are impractical to perform outside the lab setting under ideal conditions.

I recommend you place a two different kinds of seals on each part of the case. Ensure that you cover the front, back and sides with seals. After securing the machine make sure you cover the keyboard. There are websites devoted to selling keyboards of every make and model and they have key logging chips inside. In fact, there are even used keyboards to complete the subterfuge. Seals (with serial numbers) do more than prevent them from being opened, they prevent substitution.

Cables can be marked distinctively with an UV pen. Although I am unaware of any attacks being performed against the cabling, it's cheap insurance. In fact you can sign the seals with a UV pen. The ink dissolves on contact with many solvents and represents an extra layer of discrete security. You can verify the authenticity of your equipment with a simple UV LED and it can be used to prove the equipment is yours should it be stolen.

Be sure to examine the keyboard connectors on the keyboard and computer system to ensure an attacker has not secretly installed a keystroke recording device between the cable and the system housing. Keystroke recording devices are a serious security risk and you should check for their presence regularly.

PS. The DOD actually considers a good holographic serialized seal as tamper evident as a very high quality lock that would cost hundreds of dollars!

Threats you never thought existed but are still easier than Cryptanalysis.

The following are some real world extreme attacks against hardened systems. Generally, the only way to defeat string encryption is to cheat. Hiring a cat burglar to put a key logger on a computer is infinitely easier than brute force cryptanalysis. Also bribing someone $50,000 for the keys to your encryption would be a tremendous savings compared to cryptanalysis of the 128 Bit Triple DES and AES military grade ciphers commercially available. Interestingly enough nearly everything on this list is rendered moot if you

- Keep your secure computer offline (Apple machines are excellent), use a different one for the Internet,

  this is called an air gap. A hidden away encrypted laptop is 1000x more secure than leaving controversial written material for the government to find.

- Use strong password based software encryption.

- Use strong hardware token based encryption.

- Put tamper seals with serial numbers on all hardware and (ideally) lock the computer in a safe.

- Use high security Medeco brand locks on the door to your computer room. (prevent sneak ins)

- Check for hidden transmitters ("bugs") in the room you operate in.

- Work in a room that doesn't have a window.

- Burn hard disks, CD's, backup tapes before discarding them.

- Laptops are best because they are EXTREMELY portable and easily locked in safes or hidden.

So what COULD “they” do?

In order of likelihood

Break in (or barge in) and secretly (or blatantly) copy the data from your hard drive (or steal the hard drive) onto a portable hard drive and sneak out (or walk out) with a copy of your data to read plain text or analyze for weak passwords, etc. Also looking for sticky notes with passwords on them, etc. This attack is devastating and extremely successful. This is the number one attack performed by private investigators, hackers, law enforcement and spouses.

Replace your keyboard with a bugged version which appears identical but saves everything you type on a chip. This attack is devastating and extremely successful. This is the number two attack performed by private investigators, hackers, law enforcement and spouses. The bugging devices are inexpensive and commercially available.

Install or trick you into installing trojan horse and virus software can secretly transmit data over the internet or disables software encryption. It is believed that the FBI Cyber knight program is designed to capture keystrokes, including passwords to encrypted files, file and other private data. This attack is a real threat, software designed to compromise Windows based PC's is freely available on the commercial market.

Take discarded CD's and Hard Drives out of the trash you set outside on the curb.

Put a hidden video camera where it can observe your monitor. This attack is devastating and extremely successful. This is a common attack performed by private investigators, hackers, law enforcement and spouses. The bugging devices are inexpensive and commercially available.

Listening to the different sounds made when striking different keys on the keyboard and using spell check software to error check. This attack has been performed in the field by intelligence agencies against typewriters since the 1970's at least. Graduate students have released source code permitting anyone to exploit this security issue.

Putting a transmitter in your monitor / keyboard. This is a practical attack for anyone who can substitute or open up your computer hardware.

Trojan horse and virus software that secretly transmits data via the LED's on your keyboard. This attack is not known to have been performed in the field, currently this is a demonstrated hypothetical attack.

Passively reading the data from blinking LED status lights on computers, printers, etc. This attack is not known to have been performed in the field, currently this is a demonstrated hypothetical attack.

Actively transmitting data via TEMPEST signals (computer generated electronic radio noise) out of your computer after a virus or trojan horse program compromises it. This is a demonstrated hypothetical attack. There is even a free program that will play music that you can listen to via AM radio. (see Eliza for Tempest) NOTE: Tempest attacks are rare and difficult to perform.

Passively listening to electronic "noise" that comes out of your pc. (TEMPEST) These attacks extremely rare, require very special equipment and require the attacker to be physically close by. These attacks are only performed by federal agencies in major cases, usually foreign espionage. Operate in a metal box (faraday cage) to defeat this attack. Working on a laptop in a closed shipping container would offer outstanding protection. Lookup more information about TEMPEST on the Internet.

Thank you for reading our first edition

I hope you enjoyed reading the first edition of the PARANOID NEWSLETTER as much as we enjoyed writing it. We know we just might sound a little out there but think of what George Washington would say if he were alive today! The government is corrupt, evil and is constantly playing the “Terrorism” card to pass illegal laws. We need your support to continue operating. The Newsletter in paper form is always five pages printed on both sides. This is the weight limit for first class mail, priced at .44 cents. If you give us your email address we would be happy to give you the newsletter at absolutely no cost. Since it's free to send it we'll pass the savings on to you! If you are a real supporter of our work however, please ask where to send a donation anyway because we need to get the message out and sending first class mail to potential readers does cost money.

Are you a low tech person? Want the newsletter in paper form? A fifteen dollar donation will keep you in a years supply of the newsletter. We would really rather give it to you in the email format, its a lot less work and expense. You probably have a lot of specific questions and we would be happy to answer them the best we can. Send us an email and your question will be answered and included in the next newsletter. If you would like to buy anything we mention, please email us and we will give you an exact point of contact for the product.

It's not an accident that you received this newsletter. For whatever reason, we believe you would be interested in our newsletter. This is the only copy you will receive unless you contact us. Please pass this information on to everyone with the intelligence to appreciate it.

Tremendously valuable resources

Resist.com	http://www.ncmilitia.org/spycounterspy/
Howtobeinvisible.com	http://www.backwoodshome.com/articles2/wood115.html
http://www.martykaiser.com/report~1.htm	https://thementalmilitia.com/forums/

Sure you can trust the government, just ask an Indian!

We work with a separate organization that allows us to maintain our privacy and acts as a cashier to any donations. Please refer to THE PARANOID NEWSLETTER in all your correspondence, otherwise the staff will confuse your correspondence with another newsletter. Send email to TM_Metzger@yahoo.com (Note the “_” character is not a space) or send us snail mail with your donation and request for additional newsletters to:

Tom Metzger
P.O. Box 401
Warsaw, In 46581