The PARANOID Newsletter

Because they ARE out to get you.

A fool and water will go the way they are diverted. - African Proverb

Not to know is bad, not to wish to know is worse. - African Proverb

Introduction

This is the fifth 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! This fifth edition of the paranoid newsletter continues where our third edition on defeating FBI surveillance techniques left off. This current topic will continue into our next edition of the Paranoid Newsletter.

Handling the everyday risks of leading a double life.

The heroes and heroines of the American Revolution held the deep conviction that everyone everywhere has *the right* to revolt against tyranny and oppression. Many Americans today are wondering if they should become active in resisting government tyranny. Some are asking themselves, *Do I love my country but fear my government?* Answer one question and you've answered both. ...

The element of risk

Is there risk involved? Yes. Anyone who questions or challenges the status quo is a target for surveillance and repression by the authorities. Anyone who undertakes covert actions must accept an even greater risk. Your primary duty as an underground activist is security. You must remain unknown to the adversary's forces – and to the public at large. Simply stated, *exposure* is the greatest threat you face as an underground activist or as an urban guerrilla. This risk falls into three categories. ...

Sources of risk

Commonplace, everyday situations are the main source of risk. Many people are surprised to learn this. The three main causes of exposure are first, *being in the wrong place at the wrong time* (when the police are looking for someone else); second, *being noticed by the security service* (while they're watching someone else); and third, *being reported to the authorities* (by a busybody or a nosy neighbor). Reduce or eliminate these three situations and you've removed 98% of the danger in leading a double life. ...

This article teaches you how to minimize the risk of the double life you must lead. The article contains enough background information to keep you out of the internment camps. Combine it with the other articles in

the paranoid newsletter, and you'll know enough to begin planning and carrying out covert actions.

Threat #1 – The wrong place at the wrong time.

The threat involves being inadvertently and innocently swept up in an investigation. You're simply in the wrong place at the wrong time when the police are looking for someone else. When you're this close to them, arouse their interest and you're finished. Situations can develop around you unexpectedly. They can get out of control even quicker. They include mundane events like random vehicle stops by police. More serious situations include muggings, holdups, shoplifting, drunk-driver road checks, prowlers, burglaries, retail video cameras, and others. All of these situations will bring the police close by.

Case Study #1. October 1998

I was scheduled to meet a clandestine contact. The location was the entrance to a city park just after dark. I arrived ten minutes early in order to give myself time to check for surveillance. The park is laid out as a linear trail. It meanders through various neighborhoods in the city. Unbeknownst to me, just moments earlier a punk had held up a nearby convenience store. He used the trail for his getaway. I parked my car, walked to the meeting location, and checked for surveillance. Satisfied that the area was clean, I was walking back to my car. Suddenly, out of nowhere, a large dark sedan pulled out of the shadows. A male got out of the car and crept along the dark side of a building adjacent to the park. He hadn't seen me. I was thinking perhaps it was a prowler, burglar, or drug-related situation.

A challenge in the dark. As I approached my car, the suspicious male shone a flashlight on me. He was about 25 yards away. Using a firm voice, I challenged him, *"Can I help you with something?" "It's thepolice." "Oh, sorry,"* I called back. *"I didn't recognize you."* I started walking towards him in a nonthreatening way as if I had nothing to hide.

Sitrep. I had a number of things going for me. I was well-dressed. I was wearing a sports coat and tie – somewhat overdressed for the park. And I had just reacted in a manner that suggested I was not going to accept being challenged by a stranger in the dark. All these factors may have reduced the cop's suspicions a bit. As he and I approached each other in the dark, he came right out and told me that he was checking the park as a possible getaway route of the robbery suspect. I played my cover and began acting worried. *"Gee, thanks for the warning. I was just in there."*

Summary. Picture it in your mind. It's just him and me. On a deserted street. In an industrial area. After dark. He's all *pumped up* looking for an armed robbery suspect. It wouldn't take much for things to get out of hand.

His next move. Following standard police procedure, he now needed to rule me out as a suspect *and* find out what I was doing. After all, here I am hanging around a park after dark. He asked for identification. I showed him my driver's license. Then he asked what I was doing. *"I'm going down to [name of bar] to sing some Karaoke,"* I replied, looking at my watch. It was twenty to nine. *"It doesn't start 'til nine,"* I continued. *"So I'm just killing a little time."* He smiled. Then he handed back my ID and he said, *"Well, you're not 24. Have a good night."*

Home free. We can safely assume the robbery suspect was described by the convenience store clerk as a 24-year old male. I'm fortyish. The lesson? You simply never know when circumstances are going to overtake you. You cannot predict when you're going to be challenged by the authorities. Plausible denial is the best way

to ensure that a routine challenge doesn't escalate into a major confrontation. As an underground activist, you *must* have an innocent explanation for *everything* you do. In my case, I also had a *backstop*, which is spy-talk for an actual event that backs up a cover story.

Tell the cops what they want to hear. Help simplify their job for them. Play your cover for all it's worth. Be a stereotype. Make it easy for them to label you, to pigeon-hole you, to typecast you – and they'll rule you out as a suspect. I was just some naive *dandy* on his way downtown to sing Karaoke on a Saturday night. Yeah, right.

Give them what they want. An important component in your plausible denial and your cover is to give the authorities something to *"find"*. Let them discover a personal character weakness or a minor transgression. They'll seldom look further. Intelligence agencies like Britain's MI.6, Germany's BND, France's DGSE, and Russia's KGB (now SVR) have been doing this for decades. It's called *layered security*. The damage? None. I simply rescheduled my rendezvous with my contact, a whistleblower in an alphabet agency.

Summary

Threat – Unexpected police challenge.

Defense – Plausible denial. Good cover. Layered security. A backstop.

Implementation – Dress well. Be clean and neat. Be polite. Play out your cover. Become a stereotype. Act nonthreatening.

Threat #2 – Being noticed by the security service.

The threat involves being noticed by the security service when they are actually watching someone else. In other words, you inadvertently walk *through* a surveillance operation. During your meetings with various contacts, eventually you'll find yourself talking to someone who is under surveillance. The surveillance team will want to know more about you. The mere fact that you've contacted their target is enough reason for them to place you under surveillance. They don't have anything on you yet, but the situation is extremely dangerous for you.

A common trap. A situation like this can easily develop as a result of your routine interaction with other activists, urban guerrillas, cells, networks, couriers, go-betweens, suppliers, informants, whistleblowers, agent-handlers, and so on. Any one of these contacts might be under surveillance – vehicle, foot, or technical. The defense against this threat is to use good tradecraft.

Use the *Blunt-Modin* method of arranging secret meetings. Use dead drops. Use anonymous email accounts. Use one-time pads. Learn to recognize the warning signs of surveillance. Use elliptical conversation. Use diversions and decoys. Use misinformation. Use codewords. All these skills make it possible for you to continue your underground work while under surveillance. Most important, however, is your *cover*. You want to appear as one of the unthinking sheep. Make yourself uninteresting to the surveillance team.

Failsafe. Even if you don't detect the presence of the surveillance team, *good tradecraft* and a *good cover* will keep you free. The goons will watch you long enough to satisfy themselves that you're not a suspect – and then they'll move on. The cardinal rule is *don't break cover*. Ever. Let them hear what they want to hear – *a sheep*

bleating. Let them see what they want to see – *a sheep grazing*. Help them rule you out as a suspect.

Case Study #2. August 1998. One of my regular contacts was under intermittent police surveillance. That's because she has occasional contact with nasty underworld types. She and I discussed *nothing* by telephone. We use only *random* parks and noisy bars for our conversations. Sometimes we used cutouts and go-betweens to pass messages to each other and set up meetings. My cover was that of a naive *dandy* who was hopelessly infatuated with a *"bad girl"*.

Layered security. As in the previous risk analysis, it's important to realize that an essential element in your plausible denial and your cover is to give the authorities something to *"find"*. Let them discover a personal character weakness or a minor transgression. They'll seldom look further. Intelligence agencies have been doing this for decades... because it works.

Summary

Threat – Noticed by security service.

Defense – Good tradecraft. A credible cover. Layered security.

Threat #3 – Being reported to the authorities.

The threat involves being reported to the authorities by a busybody or a nosy neighbor. These so-called *anonymous tips* happen a lot more often than people realize. The threat is from the passerby, the bystander, the witness, the jilted lover, the jealous coworker. This is one of the most dangerous threats to your double life, but it's also one of the easiest threats to neutralize. The answer? Good cover and plausible denial. This means looking like *you belong* – and having an innocent explanation for whatever it is you're doing.

Your public persona must provide adequate cover for the activities of your underground persona. Of course, this only works if you keep your mouth shut. Don't brag about your activities to friends or lovers. Don't engage in *pub talk*. Unless you're among cell members, keep your political opinions to yourself.

Case Study #3. The research that I undertake during my investigative reporting for the *Spy & CounterSpy* website provides good cover for the *"serious"* contacts I need to make. My research activities provide plausible denial while I meet or communicate with informants from alphabet agencies, whistleblowers from government departments, activists in underground organizations, confidential sources in law enforcement and the media, tipsters, ex-military types, ex-spooks, and so on. What we *really* talk about is between me and my contacts, of course. With a little thought you can exploit *or create* activities in your lifestyle that provide good cover for the things you'd rather be doing.

Summary

Threat – Reported to the authorities.

Defense – Good cover. Be part of the community. Fit in. Be friendly. Be a stereotype. If possible, have a solid backstop.

Comments on Weeding out informants and agent-provocateurs.

Assessing the risks. It is imperative that you run tests to verify the reliability and integrity of new recuits who are applying to join your cell. Failure to evaluate recruits will result in your group being penetrated by your adversary – much like the militia groups in the USA have been penetrated by the FBI. Every time you admit a new recuit into your cell you are risking the security of your group. Yes, the recruit might be a *bona fide* supporter of your cause – or he might be an informant or an agent-provocateur.

The Informant. The informant is a cell member who is providing information to your adversary. He may betray you for money. She may betray you because she is being blackmailed. He may betray you because he is unethical, immoral, and weak-willed. She may betray you because she has a passive-aggressive personality disorder.

The Agent-provocateur. The agent-provocateur is someone who feigns enthusiastic support for your cause while enticing you to commit acts that are illegal. She is acting on the instructions of the FBI – or she may actually be an FBI agent. You are being set up for arrest, interrogation, and conviction.

The Mole. The mole is a cell member who quietly works to sabotage your operations. He may deliberately *forget* to do things that result in failed operations. He may intentionally *ruin* meetings with specious arguments and pointless debate, often introducing paranoia into the discussion. A typical mole is a long-time cell member who has been recruited by the FBI, perhaps by blackmail. Less frequently the mole is an FBI agent who has penetrated the organization at an early stage in its development.

The Counterintelligence Role. It is vital that your organization have a *counterintelligence officer*. This is someone whose role is to detect and neutralize attempted penetrations by the enemies of your organization. Whether this is a formal position or an *ad hoc* role is not important. Someone in your group must take steps to systematically and conscientiously evaluate new recruits. If you don't make an effort to defend yourself against penetration by your adversary, then you'll end up like the militia groups in the US... paranoid, disorganized, ineffective, and – more often than not – in custody.

How to Uncover informants. Here is how established resistance movements uncover informants. First, reveal some sensitive information to the recruit – and *only* to the recruit. For example, you might inform him of the existence of a (bogus) hidden cache of weapons. Then wait and watch. If the cache is suddenly discovered by the authorities, you may be dealing with an informant. More tests may be required to confirm your suspicions.

In serious cases where you're playing by Big Boys' Rules, you might need to use live bait. If your adversary is sophisticated and experienced, you might need to reveal genuine secrets to the recruit you're evaluating. For example, you might reveal the name of a *whistleblower* who is leaking information to you about your adversary. If your recruit betrays your information to your adversary, you'll have lost your whistleblower – but you'll have unmasked an informant before he can do too much damage.

Unmask an agent-provocateur. Here is how any organization can unmask an agent-provocateur. If the person is full of ideas for future operations, then *insist that he lead by example*. Make him commit himself first. Or, to put it another way, make him incriminate *himself* first before asking others to risk injury, exposure, or arrest. If the person balks, then he may simply be "all talk". Or he may be a coward. Or he may be an agent-provocateur. In either case, you've called his bluff and now you know not to fall for his *jive-talk*.

Enforce compliance. Here is how resistance movements enforce compliance with the counterintelligence functions. If a trusted cell member brings an outsider into your group – or reveals sensitive information to an outsider – without performing any of these counterintelligence measures, then that cell member must be severely disciplined. Depending on your situation, simply ostracizing the individual may suffice. Punishment ranges from revoking his membership to revoking his birth certificate.

How to setup a dead letter box

Traditionally, deep-cover agents pass messages, documents, money, weapons, and other material between each other without compromising their security using dead letter boxe's. Neither agent knows the identity of the other. Nor do the authorities know what's going on. The method described in this article has been used by foreign intelligence agencies and underground groups to thwart the counterintelligence and counterespionage sections of the FBI. A dead-letter box (British English) is also called a dead drop (American English). A DLB is a physical location where material is covertly placed for another person to collect without direct contact between the parties.

Good locations for dead-letter boxes are nooks and crannies in public buildings, niches in brick walls, in and around public trash receptacles, in and around trees and shrubs, a third-party's mail box, between books in a public library, inside the paper towel dispenser of restaurant washrooms, and so on. The key to success is ingenuity. If the item being passed can be disguised as a discarded candy wrapper or hidden inside a cigarette butt, etc., so much the better.

DLB Protocol. The method described in this article was originally devised and perfected by the KGB for use in Britain and the USA during the cold war. But the technique is so effective it's still in use today – and is used by more than 30 intelligence agencies and underground groups worldwide. When used by two people who have basic skills in countersurveillance, this method will confound an FBI surveillance team as demonstrated by the FBI's inept handling of the cases involving Aldrich Ames, Jonathan Pollard, and John Walker Jr.

Tradecraft. You need to know three pieces of tradecraft to make this technique work.

Trick #1 – Pick a good site for your DLB. This means choosing a spot where you're *momentarily* hidden from view while you pass by (and either load or empty the box). It also means selecting a site that is easily accessible and in a public location.

Trick #2 – Use a separate set of sites to signal to your opposite number that you're ready to place something in the DLB, or retrieve something from the DLB.

Trick #3 – Use a foolproof signal that tells both parties that the material in the site has been picked up. This guarantees that the first agent can go back and recover the items if the second agent is unable to make the pickup for some reason.

Step 1: Give the ready-to-fill signal. Let's suppose that you need to deliver a document to your contact. The first thing you do is transmit a "ready-to-fill" signal. You need to tell your contact that you're ready to fill the

DLB with your material. For example, you might place a piece of chewing gum on a lamp post at a pre-arranged location at a pre-arranged time (perhaps the second Tuesday of each month at 1:30 pm). The trick is in using signals that can be easily seen by a lot of people. This means that your contact does not have to compromise his/her security while reading your signal.

Step 2: The ready-to-pickup signal. When your contact sees the ready-to-fill signal, he/she will send a ready-to-pickup signal. Again, this signal must be sent at a pre-arranged time and location, say at 2:00 pm. It might be a chalk-mark on a traffic signpost or back of a park bench. When you see the ready-to-pickup acknowledgement, you must fill the DLB within 15 minutes (ie by 2:15 pm). After placing your materials in the DLB, you immediately return and remove your ready-to-fill signal, thereby indicating to your contact that the box is filled.

Step 3: The all-clear signal. Upon seeing that your *ready-to-fill* signal has been removed, your contact goes to the DLB and retrieves the material that you've placed there for him/her. This must be accomplished before a pre-arranged deadline, say 2:30 pm. Your contact then returns and removes his/her *ready-to-pickup* signal, indicating that the box has been emptied.

When you see this all-clear signal, you leave the area. However, if you don't see the signal by a pre-arranged time, you return to the DLB and retrieve the material in order to prevent it from falling into unauthorized hands. This system of signals can be made even more secure by using positive acknowledgement signals instead of simply removing existing signals, of course.

Providing security for your DLB. To maintain watertight security for your DLB, simply weave a number of *fake* DLB locations into your routine on a daily, weekly, or monthly basis. Narrow passageways between buildings, covered pathways in public parks, nearby dumpsters behind restaurants... all these are ideal. Simply make it a point to walk past these fake DLBs *on a regular basis*. Remember, each DLB is located such that you'll be *momentarily hidden from view* as you pass it. If you're under surveillance, the goons will go ballistic. They'll need to place an agent at each suspected DLB *at the precise moment you walk by*.

If you've chosen your sites carefully, there's no other way for the goons to monitor these locations. If you have three or four fake DLBs that you regularly walk past, you'll soon notice the *telltale pattern of strangers* who just happen to be loitering nearby at the instant you're momentarily hidden from general view. When this happens, you've detected the presence of a surveillance team. Suspend your covert activities until the surveillance passes.

SURVIVAL TIP – Even if you're not using DLBs, it's a good idea to walk past fake dead-letter boxes as a part of your weekly routine. I've caught more FBI gumshoes than I can count with this one simple countersurveillance technique. To date the FBI trainers have been unable to develop a defense against this particular countersurveillance maneuver and you just haven't *lived* until you've seen the facial expression of an FBI spook who suddenly realizes he's been *burned* by the target of the surveillance operation.

Anonymously and instantly move money via reloadable debit cards

(How the hi tech teenagers and computer nerds move money instantly)

Reloadable debit cards are debit cards that can have funds applied to them at future dates. You need an identity to get the actual plastic card activated. You should also have a safe mail box to get the card mailed to. Pretty much, you go into a store that sells the reloadable debit cards with a bunch of cash in hand. You give a clerk the money, and they give you a temporary card. The temporary card can't be used for much, it is just a number on cardboard, not actual plastic. You need to call and give an information (SS#, address, etc.) to activate the card, and then the actual plastic card is mailed to you.

To activate the card, you should clearly not use an info that has ties to you. You also should not use a phone that has ties to you. Disposable prepaid cell phones are good for this. Also, you should have the card sent to a box registered with a fake ID, or an abandoned house or some such thing. Naturally, there should be nothing to connect you to the debt card.

Although you need a secure place to receive the plastic card, it is very easy for people to send you money. They merely need to go into a store that sells reload packs, and hand the clerk some cash for one. The clerk loads the cash onto the reload card. Now, they can take the number off the reload card and send it to the person with the plastic card. The reload number should be sent encrypted in all cases, in the event law enforcement is monitoring your communication. You do not want to get a persons card flagged, nor do you want to draw attention to yourself.

I suggest people refuse reload card information that is sent to them without encryption. The person with the plastic card can now take the number of the reload card, and can use it to apply funds to their plastic card online. This should be done behind anonymous proxies in all circumstances! Green dot reloadable cards are only sold in the USA, but different countries are likely to have different reloadable cards. Parts of Europe, including Russia and I believe Germany, have Web Money Cards, which are like a mixture between reloadable debit card and E-currency.

When cashing out money from a reloadable debit card at an ATM, a great deal of care can be taken. Gloves should be worn, as should hats and long sleeved clothing. The plastic card should be free of fingerprints, some ATM machines can 'grab' cards, which could later be forensically analyzed. You should park at least a block away from the ATM you use, a better bet would be to use a taxi and be dropped off a block away from the ATM you plan to use. **ALL ATM MACHINES HAVE HIDDEN SURVEILLANCE CAMERAS INSTALLED.**

There are creative payment schemes can be created reloadable debit cards. Someone trusted with access to lots of identities and boxes can get cards in bulk, and resell them once they are activated. People buying pre-activated reloadable debit cards do not need safe boxes or access to identities, they just need a magstripe encoder and blank card stock. Here is the scenario:

One person gets many activated reloadable debit cards. They use a skimmer to get dumps of the magstripe information. Skimmers are usually used by people who commit credit card fraud. Essentially, they

make a perfect digital copy of the information on a cards magstripe. The person can take this dump and encrypt it to a customers encryption key, then encrypt the card dump. The person buying the activated reloadable debit card then decrypts the dump and uses a magstripe encoder to encode it to a blank card stock. The blank card is essentially the activated reloadable debit card now, as far as an ATM can tell.

For this system to work, the person selling the activated card information must be trusted to not keep a copy of the card themselves. If they keep a copy of the card, they could steal money intended for you. If they are trusted and destroy their copy of the card after selling it, this can be a good market for people with access to identities and boxes, and a great way for people to buy anonymous ATM cards that are easy to fund for customers.

Reloadable debit cards should be split up over regions. Time should be allowed to pass between funds being added and money taken off them as well. Remember, reloadable debit cards are not designed for money transfers they are designed to be used as actual debit cards. If the company providing the reloadable card sees it is being loaded by people over a wide area, and the money is immediately cashed out at an ATM, they will likely freeze the card and the assets loaded to it. For this reason, I suggest you use specific reloadable cards to cover different regions of the area you work. Also, if you only work regionally, reloadable debit cards can be the perfect solution. You should not move more than around $1,000 a month through a single reloadable debit card, or you risk it being frozen.

Don't forget to remove the hidden info stored by digital cameras in JPEG images.

Modern digital cameras encode information about the camera in the jpeg images they create. The first thing we will discuss here is Metadata. Metadata is quite literally data on data. There are various forms of metadata, and it can reveal a lot of information you are probably wanting to keep secret. Let's say you take a picture with a digital camera, and then load it to your computer. If you use the JPEG format, a lot of information is going to be available in your picture. Such information will likely include some or all of the following:

Camera manufacturer, camera model, camera serial number, software used, time of photograph, flash status (did the flash go off when picture was taken) and other technical information.

Now a lot of things can be done with this information. If you post a picture, even from behind an anonymity network, it isn't going to be very anonymous if the picture has the serial number of your camera attached to it with metadata. Perhaps you registered the camera for a warranty, and it will not be trivial for law enforcement to find your true identity. Even if you did not register the camera, often times the serial number can pinpoint the store you bought it from, and in some cases you may still be on CCTV surveillance cameras buying it.

Even if the meta data does not contain your serial number, simply leaking the manufacturer and model of the camera can be used as circumstantial evidence against you after you are raided and the camera is discovered. Software used can leak information about your operating system in many cases, which can be used against you in several different ways (including targeting specific exploits, rather than guessing which OS you are using).

Time of the photograph can help a forensic time line of activity be built and presented against you in court. Sometimes there will be a thumbnail of the photograph stored in metadata, and even if you edit the main photograph the thumbnail will stay the same. So perhaps you have a photograph that reveals information on yourself in part of it, and edit that out. With out removing metadata, you could be at risk of a forensic scientist recovering the information you removed from the picture by analyzing the metadata thumbnail. In other words, a lot of evidence can be gathered on you from a simple digital photograph.

There are a few ways you can remove metadata from photos. One way is to load the photo with metadata to your computer, and then view it full size in a photo editing program. Now hit your print screen button on the keyboard, which is usually right after F12. This takes a screenshot of your desktop. Since the full sized photograph was viewable on your desktop, it takes a screen shot of the photograph. You can now cut out the photograph from the full desktop screen shot, and save it. The newly saved image will not have any metadata attached to it, and you can securely erase the old image.

This trick should work for all formats of images. There are various programs that allow for the removal of metadata from photographs as well, which can come in handy if you want to sanitize a lot of your images and don't have time to take a print screen of each one. I do not know of any such programs off the top of my head, but you will find an abundance of them if you look.

You should also know that the blur function of your image editing program is almost certainly inadequate. Forensics can unblur things pretty easily, the algorithm to blur pixels does not use cryptographically secure number generation and as a result, forensic analysts can reverse engineer the blurring. You need to actually go over the identifying marks with a paintbrush or cut them out, at which point you should likely take a print screen of the edited image. Now cut the image out of the print screen and paste it as a new, edited image.

Microsoft Office documents (such as spreadsheets, presentations, text documents, PDFs) are other sorts of files that can have damning metadata. Document metadata often includes:

The name of the account the document was made in

Name of the company the computer that made the document is registered to

The name of your computer

The account names of people who previously worked on the document

Document revisions

Document versions

Amount of time spent editing the document

As you can see, there is a variety of ways that office file metadata can be used against you. If your computer or account is named after yourself (as many people do), then you could very well be publishing your real name when you publish your sensitive documents. Perhaps the location of your place of work can be determined. Chains of custody can be determined in some cases, meaning if you send a document to someone else people who find the document and analyze the metadata can determine it came from you, and also where

you got it from (or if it originated at you).

There are a few things you can do to minimize the damage of office file metadata. First of all, you shouldn't be using a computer or account named after you in the first place, and you shouldn't be using software that is registered to your name. Second of all, you shouldn't ever do sensitive things from a work computer that has ties to you (although cafe computers can in some cases be ok if you are not directly linked to them). Third of all, after you finish creating an office file, or after you get one before forwarding it on, you should copy and paste the information to a new document and securely erase the original. This will remove some metadata (versions, revisions, time editing, previous authors, etc), but not all of it (computer name, account name, company name, etc).

There are also software tools to remove metadata that you should make use of. The program you use will depend on what type of document you are cleaning. Microsoft has a free metadata remover for Microsoft office documents. I imagine it is probably fairly trustworthy, simply because they intend it to be used by lawyers and such to remove metadata that could leak confidential information. You should be able to find a free program to remove metadata from whatever sort of office document you are using, just use a search engine.

One more specific note on PDFs that certain people might find helpful; simply covering words with black boxes usually won't actually erase them. You can highlight them with the mouse even if they are under the blacked out bits, and then paste them into a word document or some such thing. This exploit was used against a US military agency that released a document with confidential information incorrectly blacked out, and lead to leaking of sensitive information. This is similar to metadata, but isn't. Plain text files are the simplest kind of document format and contain no hidden data whatsoever. These files have the ending .txt and they look like typewriter text. Various fonts, bold, italics, etc. are not possible with this format.

Another sort of metadata on your computer is general operating system created metadata. This can include such things as timestamps (file creation data, last accessed, last modified, etc). It is probably not much of a stretch to call information stored by the OS in places such as the registry as metadata either. Such information can include a great deal of things you likely would not expect. For example, Windows XP keeps a hidden log of every website you have ever visited with internet explorer since the installation of your computer, it also keeps various other data logs including the names of programs you have launched and the dates you launched them.

There are Windows XP tutorials that demonstrate how to disable to built in Windows XP metadata (forensics) tools. Timestamps alone can be very damaging against you. In addition to helping to form a timelines, they can be used to counter defenses in court. Microsoft goes out of its way to design its operating system in such a way as to leave forensic evidence everywhere! Switch to a difference operating system like OS X (Apple) or one of the various Linux based operating systems. OS X is the easiest for inexperienced computer users. Unfortunately, you will have to buy an Apple computer to use OS X. The Mac mini is the least expensive machine offered by Apple and you can use your existing mouse, keyboard, monitor and other accessories.

Don't forget that most color printers encode microscopic yellow dots into the paper that is printed on. The yellow dots are arranged in a way that is unique to each printer. They reveal the model and serial number of the printer they were printed on. This makes it quite easy for someone to positively connect a printer to a certain printed document. This is done at the request of the Secret Service to link counterfeit money to a particular printer. Printer manufacturers do not deny this. Extensive information on this subject is available from the Electronic Fronter Foundation. **http://www.eff.org/issues/printers**

Thank you for reading our fifth edition

Visit Resist.com to buy future and archived editions.

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 for sales and 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