Your Privacy Manual

Bill Rounds, Esq.
Trace Mayer, J.D.

Table of Contents

BONUS MATERIAL

LEGAL DISCLAIMER

This book is intended to be a general discussion only, and must not be considered legal advice. Your use of it does not create an attorney-client relationship. Any liability that might arise from your use or reliance on this book is expressly disclaimed. This book is not legal, loan, accounting or tax advice, and is not to be acted on as such. All readers are advised to seek services of competent professionals in the legal, business, accounting, and finance fields. References in the book to products, service providers, and potential sources of additional information do not mean that I can vouch for such products or services or the information or recommendations in those sources. I am not responsible for any third-party product or service or content over which I do not have control.

Introduction

> I think judgment matters. If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place. If you really need that kind of privacy, the reality is that search engines -- including Google -- do retain this information for some time and it's important, for example, that we are all subject in the United States to the Patriot Act and it is possible that all that information could be made available to the authorities.
>
> - Eric Schmidt, Google CEO, 9 December 2009

The issue is not security or privacy but instead freedom of choice or coercion. Violence and intimidation, whether it arises from a foreign attack or from domestic authorities with their police state microscopes focused on everyone's lives, the effect is the same: tyranny. Freedom of choice, that which makes life worth living, requires as a fundamental element for the individual to securely go about life without intrusion or the threat of surveillance. Where there is ubiquitous police surveillance there is the police state. Therefore, if we value freedom of choice instead of coercion and force then we should be staunch advocates for privacy, especially when we have

nothing to hide.

If we are espied in all circumstances then we are persistently under threat of being unjustly judged, criticized, corrected, punished and even plagiarized of our own autonomy. We become wards of Big Brother, bound in the chains of coercion with the reasonable fear that, either now or when we least expect it, any action may later become evidence for some imagined wrong because the All Seeing Eye observes and records the minutia of daily life.

Thus, without the ability to keep secrets, individuals lose the capacity to distinguish themselves from others, to maintain independent lives, to be complete and autonomous persons. This does not mean that a person actually has to keep secrets to be autonomous, just that she or he must possess the ability to do so. The ability to keep secrets implies the ability to disclose secrets selectively, and so the capacity for selective disclosure at one's own discretion is important to individual autonomy as well.

Secrecy is a form of power. The ability to protect a secret, to preserve one's privacy, is a form of power. The ability to penetrate secrets, to learn them, to use them, is also a form of power. Secrecy empowers, secrecy protects, secrecy hurts. The ability to learn a person's secrets without her knowledge — to pierce a person's privacy in secret — is a greater power still.

And yet it is ideas that move the world and ideas may only be supplanted by other ideas. Ideas are bulletproof. But those with inferior ideas, those barbarians who have to rely on force of arms instead of force of logic and reason tend to lash out when they meet a superior opponent.

And how do they lash out? Although warned to abandon the idea under threat of force, Galileo Galilei refused and was found guilty being vehemently suspect of heresy and confined to house arrest for the rest of his life. Why? Because he spread the rudimentary idea that the earth revolved around the sun; dispelling the Establishment's enslaving illusion.

Nicolaus Copernicus waited decades before he published the work that laid the foundation for Galileo because of the threat of criticism and force. But legend has it that the first printed copy of De revolutionibus was placed in his hands on the very day that he died, allowing him to take farewell of his life's work. He is reputed to have awoken from a stroke-induced coma, looked at his book, and then died peacefully. How would humanity have been better off if

these geniuses had the ability to keep their identity private while spreading the supernal and truthful ideas?

Yes, humanity occasionally takes detours as it climbs from the swamps of tyranny to the celestial stars of freedom, peace and prosperity. The out of control and insane governments with their costumed stormtroopers are becoming destructive of the ends of safety and happiness of the heirs of the Founding Fathers and of the whole world. Is it any wonder that China requires the identification of anyone who uses the Internet?

But it is the right of those heirs of freedom and liberty 'to alter or to abolish it, and to institute new government'. Ideas will spread. Coercion, force, theft, fraud and all manner of immoral behavior, whether done by the authorities or anonymous criminals shrinks and withers before the sunlight of truthful ideas.

While the baton, taser, assault rifle or stealth bomber may be used in lieu of conversation, words will always retain their power. Ideas can only be overcome by other ideas. Violence and force are powerless against the power of ideas and in many cases their use only hastens the spread and adoption. Words proffer the instruments to meaning. Equity, freedom, justice, peace and prosperity. These are not mere words; they are vantage points. The pen is mightier than the sword.

We want to help you exercise your unalienable right to secrecy, or in other words, to have you and your property left alone. We want you to be able to live, work and play without the constant fear of being monitored and, potentially, unjustly judged, criticized, extorted, detained or punished. Our desire is to staunchly protect and defend the individual's privacy so that you can be what you were born to be: free and independent.

You will be guided by How to Vanish in many aspects of personal and financial privacy with practical suggestions to legally protect it. Everything from the sensible, like keeping your personal data from nefarious scammers, spammers, phishers and identity thieves, to the reassuring, like securing your confidential communications, your home and your finances to ensure they are free from other's unsettling intrusions. You will learn solutions and suggestions at every level of ease or difficulty in terms of time, money or effort. No matter where you are on your journey towards privacy, except maybe Jason Bourne, you will find useful and actionable information.

You will learn principles and techniques that will help at home or abroad in avoiding the dangers inherent when privacy is breached. You can select the most applicable methods and techniques to practice. Then you can progress towards and achieve increasingly difficult goals. This journey is exciting and intriguing so be creative and have fun!

How To Vanish For Free

This first section contains several options for protecting your personal and financial privacy that are totally free of monetary cost and are also relatively easy in terms of time and effort to accomplish. These tools, or a combination of what you think are the most effective for you, are a great way to get started protecting your private information. In many cases there will be a more robust or more private option that will cost money, time or effort, but often the free tool will provide as much, and sometimes more, protection than even some of the more costly methods and tools discussed later in this book. Smile. You are about to learn some very useful and fun things about how to vanish.

Location

HOME ADDRESS PRIVACY

Your actual physical location is one of the most important things that you can make vanish. There are several strategies you can use to keep your home address private. Using a combination of these strategies to suit your needs is probably best.

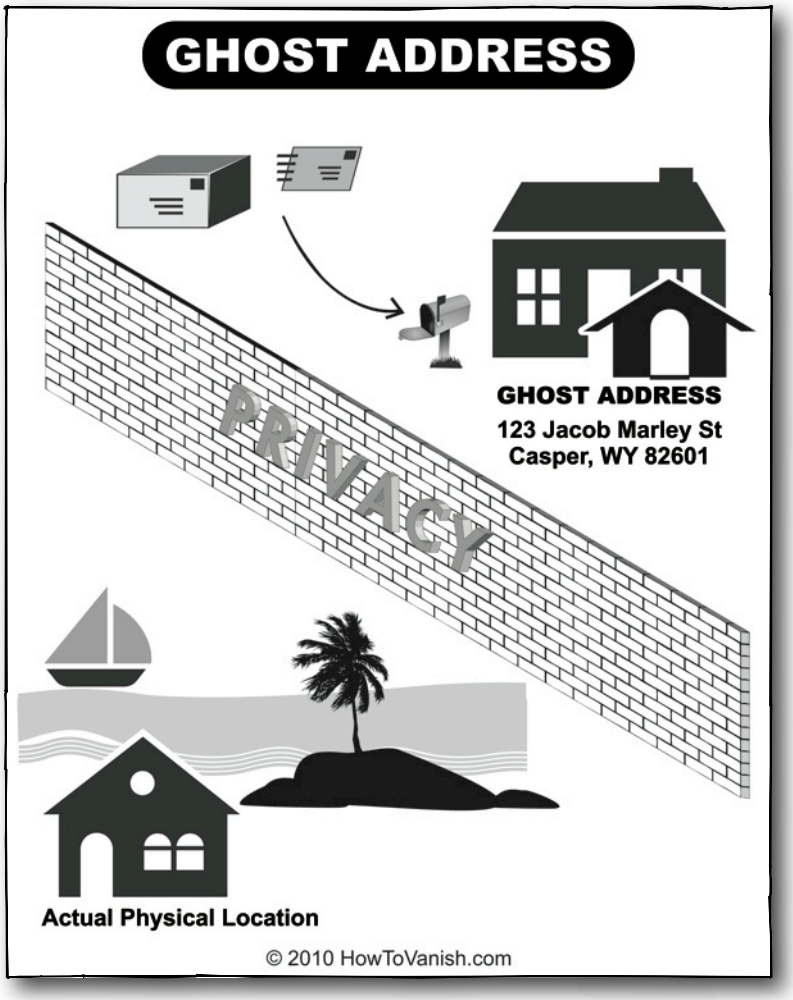
The most potent strategy, which you should use as often as possible, is to simply avoid revealing your home address to anyone except those you trust, such as your closest family and friends. When asked to provide an address on a form, leave the address field blank. If you have to give out your address to get a "free" prize, that prize is not free, it costs you your privacy. Make sure it is worth it. When you have to provide your home address to get some goods or services, consider getting them somewhere else or go without.

You will undoubtedly be asked for an address on many occasions. Unless it is a government form where your address is required, like a voter registration card, you most likely do not have to disclose your address. For those few trusted individuals who do know where you live, they should understand and be capable of protecting your privacy interests in case anyone tries to get your address from them.

Refusing to provide your address outright may arouse suspicion or may be inadequate to convince the other person not to take your address. Less suspicion is raised if you are staying with friends for a while or if you are homeless and have no address. In a tough economy, this kind of thing happens a lot. Another possible situation are those who have recently moved to the area and have not yet established any permanent place to live. You may have even forgotten your address, especially if you are new or doing a little couch surfing. Ask if you can leave the home address blank for now on a form, even if you have been told that the address is required. If you are able to continue at that point in whatever errand you were doing then there is little chance that you will need to reveal the address later.

There are many times when a physical address will be required for what you are trying to do. A third way to avoid revealing your home address is to use an alternate address, sometimes called a ghost address. For example, you can have a friend or family member receive mail, packages or messages at their address. This is especially useful if you move often and you always need a permanent place where you can be contacted. Use their address any time you need to provide a permanent address. Be sure to get their permission first, you may soon become the least favorite sibling if you don't.

If you have not practiced keeping your home address private in the past, moving provides an opportunity to start fresh and then keep your new home address private from day one. Do not fill out a change of address form when you move. You should contact each person or business that needs your new



address individually. If you won't be moving any time soon, you can fill out a change of address form and have mail forwarded to one of your alternate addresses or ghost address. In many cases, it is possible to go paperless and receive all billing and account updates online. This allows you to get important notifications by email, which can be accessed anywhere in the world, rather than require delivery to your secret hide-out and lets you save a tree at the same time.

You can go as far as signing up for free newsletters or some other junk mail services in an assumed name or pseudonym at your current location to make it appear to anyone who intercepts your mail that there is another person at your actual address, especially because this name will appear in databases and other public places. This will kill the tree you may have tried to save.

If you have UPS or FedEx or even pizza deliveries to your home address, always have them delivered to a business name, a friend's name or a pseudonym and not your own name. It is even better to have packages delivered to an alternate address. You can also protect your privacy by having deliveries made in your first and middle name, or some other combination of your name, rather than your regular given name.

COMMUNICATIONS

PHONE PRIVACY

First, keep your number unlisted. Ask your telephone service carrier to unlist your name, address and phone number from its directories. This may require that you change your number. To remove your number from Google listings, query your own phone number. Click on the phone book results and then click on remove your results from the list. Fill out the required information and Google will remove your phone number from its results.

Google Voice is a VoIP service which provides call forwarding to any US phone number, some international numbers, and has many other features. It is free if you have a Gmail account, which is also free. You are able to select a phone number in any US area code and that number never has to be tied to your real name or physical location. There are some compromises that must be made, however, if you use their services. Google Voice will keep track of what communications you make, the IP address you access your account from and

other things in the same way that they do with email. They allow advertisers to use this information to advertise when you use Google's services and may give this information over to authorities if they think they are obligated to do so. Thus their extensive records of your activities could possibly be compromised. When used in conjunction with other recommendations in this book, however, Google Voice can be very useful.

Growing up, my best friend's dad had a lot of sensitive electronic and radio equipment. With that equipment, my friend and I stumbled upon signals from baby monitors and cordless phones for a several block radius while searching for legitimate radio transmissions. Using a digital cordless phone is better than using an analog cordless phone because the signal is more difficult to intercept than an analog phone. The same is true of digital cell phones versus older analog models.

If you are ordering traditional phone service, you can register your phone under the name of a willing friend. Make sure you pay your bills in cash or money order or have the friend pay from their bank account or checks to keep your name completely unassociated with the number.

Do not leave your name on your answering machine or voicemail message. If possible, leave a pre-programmed message as the voicemail greeting because even recognizing the sound of your voice could be enough to confirm that the phone number is yours.

Your conversation is only as private as you and your interlocutor make it. If you cannot trust anyone then do not speak at all. Assuming that you do still speak to somebody, make sure that the people you speak with over the phone and in person have taken the necessary precautions to secure their end of the conversation as well. Someone may have speaker phone on while in a crowded room while you are divulging juicy secrets thinking the conversation is private. This makes for hilarious Hollywood comedy but not so pleasant privacy invasion.

There is a special precaution to take when dialing 911. Whether using a land line or a cellular phone, they already know what number you are calling from. I do not recommend giving a false name to the operator. You can tell them that you wish to remain anonymous. The number that placed the call and the caller's name are kept in the record of the incident for which the call is made. Therefore, if you must call 911 then do not give your name or call a friend and tell them to call 911 so that even your phone number is not

associated with the incident.

ENCRYPTED PHONE CALLS

The most familiar way to encrypt phone calls is to use Skype. Calls are free if you are talking to another Skype user. Just download the software and you can begin making encrypted phone calls. A more robust way to encrypt phone calls is through Zfone. Zfone offers software that can be downloaded and used with many Internet based phone call services like Gizmo or Xmeeting and is available at zfoneproject.com. Skype still has a lot of your data and is probably still subject to wiretaps by government entities like most other telecommunication services.

CELL PHONE SPECIFICS

The most basic way to protect some of your privacy when using a cell phone is to have the phone issued from a city far from your home, especially one which you never visit. Chances are that most people who will obtain your number for whatever reason will think that there is some connection between yourself and that city, such as permanent residency. This may help to convince people that you are from out of town. There are even many cell phone services which offer free long distance calls to minimize the cost of having a long distance phone. Or, you can use Google Voice to make long distance calls for the cost of using your regular minutes.

Most cell phone companies “lock” their phones so that you must use the hardware of the phone with their network. Many cell phones can be “unlocked” and you may then switch to any service you want to use as a cell phone provider. You may also use the card with the contact list and other data that you have stored in another phone without switching networks. Whether or not you can unlock the phone and the steps that need to be taken in order to unlock the phone will be different for every phone. In many cases you can simply call the service provider to get the numeric code that you need to enter into the keypad to unlock your phone. In almost all cases it is legal to unlock a cell phone and even to unlock a smart phone like an iphone (also called jail breaking).

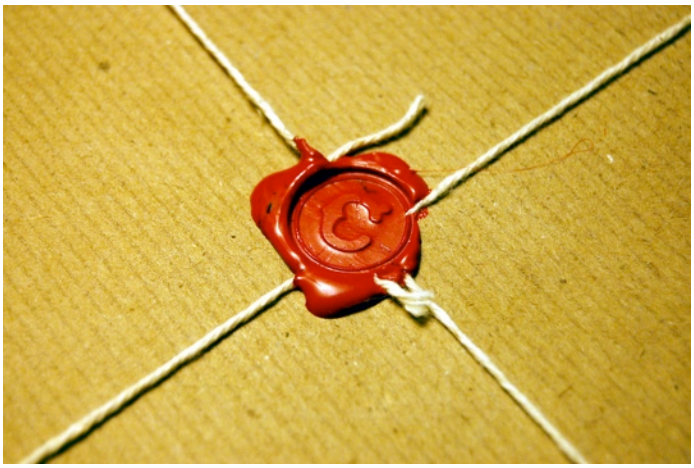
You should dispose of the SIM card when you get rid of your phone because it will contain a lot of personal data. The SIM card is tied to you like the registration of your vehicle, so if it is used later in a crime, the crime could

be tied to you. You can also follow the user manual or follow the instructions at www.ecellular.com/recycling/data_eraser to wipe out all back-up data of call history or contact lists from your phone before getting rid of it.

Remember that no voicemail box is secure because the code can be hacked. You should erase your messages immediately and urge your friends not to leave detailed information when they call. Their first name and whether you should call them back is probably all that you need.

Over the next few years, cell phones will be the main way that people's location, activities and associations are tracked. All modern cell phones now have the capability of tracking the location of the phone within a few feet. If you turn your cell phone off, the location is not broadcast to your provider and they cannot track the location of the phone. Turn it on only when making a call or when you are not worried that people might know where you are. There is a possibility that your cell phone has been hacked and is broadcasting information about you, including GPS coordinates, sound and other stored information, even when the phone is off. To avoid being monitored surreptitiously, you can remove the battery and only put it in when you are using the phone.

POSTAL PRIVACY



The front side of every envelope of all mail is electronically scanned by the US Postal Service. Omit a return address on mail that you send to remain anonymous to the Postal Service scanners. You may choose to simply place it on the back of the envelope to avoid having it scanned. Because even your handwriting may be analyzed and identify you, type out the letter on a computer and print both the letter and the address on the envelope using a black and white laser printer. Many ink and color laser printers embed an invisible code which can be traced to the printer you used. To be extra safe

you may even photocopy the original. Putting clear tape over the flaps of the envelope can prevent tampering. Use an envelope that will prevent peeking through to see the inside like one lined with foil or simply insert a piece of thick, dark construction paper into the envelope.

Try to notice if there are any irregularities in the volume of mail you receive or in the expected receipt of some piece of mail. If there is an interruption, someone may be tampering with your mail or at least monitoring what you receive.

Use codes. Codes have been used to secure communication for millennia. You can go as far as to use an old enigma machine to create your coded messages, or use a less complex code, even as simple as replacing your own name with that of someone else.

Send or receive mail at a place of business where the outgoing mail is not left unattended. Places to consider are the post office itself, your own work or a grocery store that has a mail drop. Do not put your mail in your own street side mailbox or even in the public street side postal boxes that are unattended. It is very easy, and very common, for mail thieves to follow letter carriers around and intercept mail soon after it was dropped off. It is also very easy, and very common, for mail thieves to scan a neighborhood for all the raised red flags and take all of your outgoing mail before the mail carrier takes it. You can also wait for your mail carrier and hand each letter directly to them.

Do not use a postage meter. All activity used with the meter is tied to you.

EMAIL PRIVACY

As was discovered in the 2008 US presidential campaign, an email account can be hacked by a teenager. This may be embarrassing but it can also lead to more serious consequences. There are some simple precautions that can be taken to avoid most hackers. Of course, the higher your profile, the more incentive there is to hack your email and so the more likely someone is to hack your email.

First, use password and password reminder best practices. Do not use a word that is in the dictionary as a password. The safest passwords are a random group of letters, both upper and lower case, numbers and symbols. An example would be u%Ih4rS~. This involves a trade off of a password that is

easy enough to remember and the strength of the password. You should determine for yourself where on the spectrum of ease of remembering versus strength of password you want your password to be. Do not use publicly known or easily guessable passwords or password reminders. The lesson learned from the 2008 presidential campaign was that a password reminder that is public information or one that is easily guessed, like where you met your spouse, is not much protection at all.

A common way for hackers to get your email is to replicate your email login page with a fake one and, when you log in using their fake page, you have unknowingly provided them with your name and password. If you use a very common email system like Yahoo or Gmail it is more likely that someone will make the effort to produce a replica login page because they can use it over and over again with other targets. If you use a more obscure email system, even if it is still free, there is less likelihood that replica pages will be launched to attack you.

Email is sent out into the cloud in its plain text form unless you encrypt the email. Hushmail is a free email service that does an excellent job of encrypting your emails and making their contents vanish from interceptors. It even stores the emails on its server in an encrypted format which cannot be broken unless an expert hacker with significant resources hacks it or there is a court order from the Supreme Court of British Columbia, Canada to produce those documents. The encryption only works if you are sending email to another email encrypter. If your recipient does not use Hushmail or some other method of encryption, then you still have the benefit that Hushmail does not reveal your IP address, like most other email messages will, and allows you to include a digital signature which prevents altering of your message before it reaches the recipient.

OpenPGP is a software program that is free and allows you to encrypt emails. This requires more work than Hushmail in that you must take more responsibility for its use. While Hushmail encryption operates seamlessly in the background with OpenPGP you are not limited to the small storage space of a free Hushmail account.

For infrequent, one time emails, there is also the option of sending an anonymous email to another recipient. A service like Anonymouse allows you to send an anonymous message to any recipient. There is no requirement to include a “from” email address. Thus, even though the content may or may not

be secure, the sender remains relatively anonymous.

FINANCIAL PRIVACY

BANKING PRIVACY

Banks and other businesses have very strict requirements for reporting cash transactions. Currency Transaction Reports (CTR) will be filed for transactions exceeding, either individually or in aggregate, FRN$10,000. To avoid the reporting requirements that banks and other financial and transactional institutions have, you should not make transactions of $10,000 or more, even if several transactions over the course of a few days add up to $10,000 because it may be construed as structuring, a term describing the efforts to avoid detection. In addition, these and other institutions must file Suspicious Activity Reports (SARs) with the government if they should reasonably suspect that the transaction is related to criminal activity, forcing institutions subject to this rule to err on the side of caution and make a report when it is unwarranted rather than risk not making one when they should have. These reports might be filed for a transaction that is as little as $2,000. You will not be notified that a SAR has been filed and all records of transactions reported will be kept by the institution for at least 5 years. There are many transactions which are not commonly made with cash, so if you use cash to make a large transaction, you may stand out in a way that makes your transaction suspicious to the institution you are dealing with. If your individual cash transactions are for $1,499 or less, they are not likely to trigger either a CTR or SAR.

Because banks have so many disclosure requirements, if you have to borrow money, it is probably best if you borrow from a private person, like a rich uncle. They are less likely to be a source of intrusion on your privacy. Keep in mind the old proverb that the borrower is servant to the lender. Servants have no privacy.

Another alternative to traditional banking are digital currency accounts. They allow for direct transfers between customers and thus, once you have established your account, your individual transactions are far more private than they would be with banks. For example, I use GoldMoney (mygoldmoney.com) but there are other reputable digital currencies as well. GoldMoney is free to open an account and the processing to open the account

is minimally invasive. GoldMoney complies with all "know your customer" requirements and therefore offers a limited amount of privacy in the account, but it is far better than having your assets in the United States or your home country.

GoldMoney gives allocated storage of precious metals like gold, silver and platinum with title held in the name of the account holder. You may also keep funds in US dollars, Euros, or many other currencies. The laws of Jersey, in the Channel Islands, govern the transactions and so there is a higher degree of privacy for account holders. The legal protection of bank privacy in Jersey is very high. Once your money is in the account you may transfer between other GoldMoney account holders with no record kept which is subject to US disclosure or discovery proceedings. Only the record of what funds were transferred to your GoldMoney account and what was repatriated into the US is visible without your voluntary disclosure or court order recognized by Jersey authorities. The US government, however, puts very severe pressure on foreign banks to reveal the activity account holders to prevent tax evasion, so it is possible that your activity may be revealed to the government. Although this has not yet happened with GoldMoney, it has happened in other instances.

FINANCIAL TRANSACTIONS

The best way to keep your financial transactions private is to use cash or currency. Using dollar bills or money orders leaves less information to be gleaned about the transaction. This applies to even mundane things like groceries and restaurants. The personal information that can be revealed in a credit card statement about where you shop or what you buy could be another important piece of the puzzle to an unwanted profiler. If you have the option of not printing a receipt for the transaction, and you do not need the receipt for tax purposes, then you may want to eliminate that evidence of the transaction as well. There is a risk of theft and of confiscation when you use or carry cash. For example, when you travel across international borders you may only take a certain amount of cash or you may be required to disclose monetary instruments. Any amount in excess of the permitted amount might be confiscated.

CHECK PRIVACY

Do not use checks unless you absolutely must. Checks have your bank account number printed right on them. Leave your home address and other

identifying information off of the check. If you must put an address on the check, use a ghost address, or even the address of the main branch of your bank.

Often times you are required to provide some personal information on the check. If you are paying a utilities account, do not put your entire utility account number on a check. The last few digits of the account number are all that the merchant needs. Also avoid putting your driver license number on your check. A DL number is safer, however, than a birth date or SSN.

PAYING BILLS

Have your billing statements sent to you by email rather than by regular mail. Most utilities and banks offer this service. Also, pay by direct deposit or other bill pay option that your bank may offer. This reduces the points at which your personal information is vulnerable to theft by mail.

Like many privacy issues, there is a trade off here between the physical security of your information and digital security. Doing things over the Internet creates other vulnerabilities, such as the possibility that you have a key logger installed on your computer which tracks all of your keystrokes, etc. Take precautions to avoid a breach of digital integrity.

ELECTRONIC PRIVACY

Stand up, walk around for a minute, shake out our arms and legs to get the blood flowing and your mind focused. Some of the following ideas can be challenging for non-technical people, but even the most novice computer users should be able to implement most of these suggestions with minimal time and effort.

PC

Most people use computers often. Most computers have all kinds of juicy tid-bits of personal information, even when you do not expect them to. These suggestions should be something that users of most skill levels can complete with minimal effort and significant returns.

Hard drives store information in various different locations on the hard

drive. Deleted data is not truly gone until other data is re-written in its place. Many unwanted documents or files might still be lurking somewhere on your hard drive that you thought were long gone. To increase the likelihood that new items will be written over the old files, defragment the hard drive. This also increases the efficiency of your machine. The help menu of your computer should be able to guide you through defragmenting your hard drive.

Your computer stores temporary files which may contain sensitive information. You should delete those temporary files often to reduce the risk that they can give away unwanted info. Again, you can look for deleting temporary files on your computer's help menu and follow the instructions. You should also delete your cookies and cache regularly. Keep in mind that you will lose some ease and speed in functionality of the websites you visit, but it may be worth the added protection.

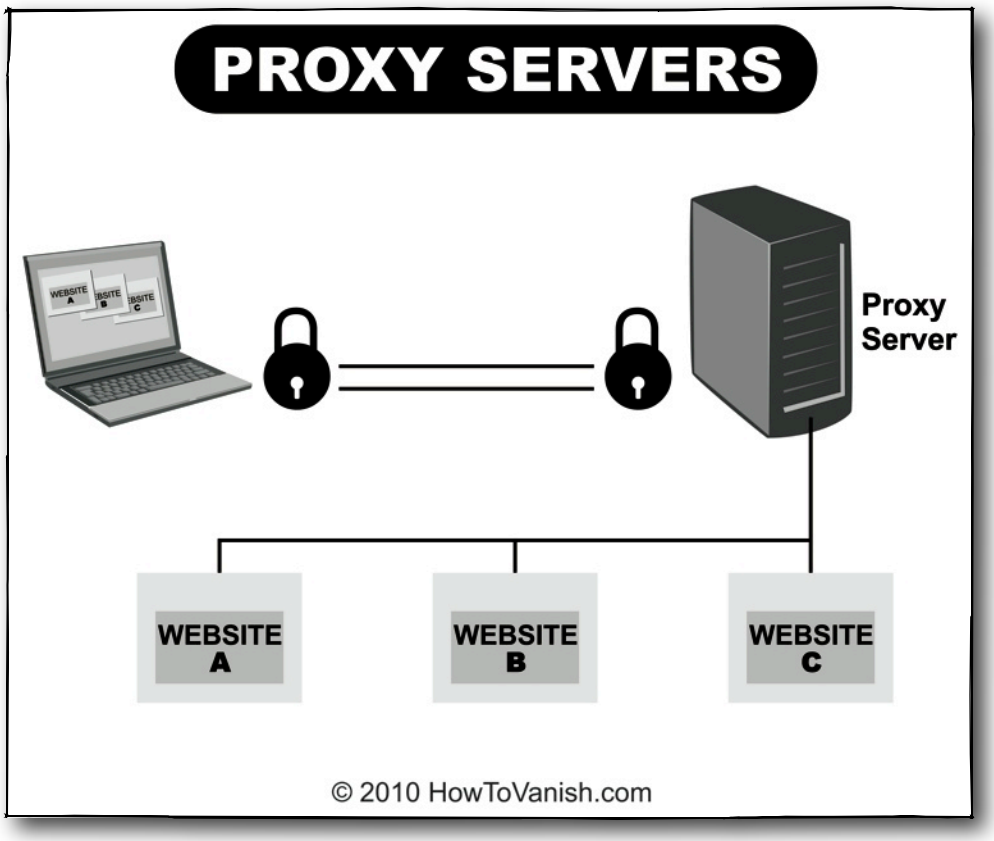
Internet service providers track your web activity and websites keep track of who is visiting them. This information is available to litigators, government officials and hackers. To keep some of your web surfing more private, use anonymous web queries like startpage.com. They do not link an IP address to the web searches done on their site, or at least the record of it is immediately destroyed after. Even so, once you click through to a website, the website will still maintain a record that you visited it unless you take other precautions.

Using proxy servers to visit websites will effectively keep your IP address unassociated with the website. The concept behind proxy servers is that you log into a proxy server, which can be anywhere in the world, through an encrypted connection and you make a request to that machine to do the web surfing for you. The IP address of the proxy will appear in the records of the websites you visit, rather than your own IP address. The proxy will then relay the information on the proxy machine to your own computer via the private connection. There are many free proxy servers available. They change often and offer many different experiences so you will want to do some research to find one that is best suited for your needs.

There are other free downloadable programs which anonymize your web

surfing such as Tor. You may also set up a Virtual Private Network (VPN) to search the Internet, especially if you are using a public access network like a coffee shop. This is more complicated than using a proxy server, and beyond the scope of this book, but if you already have the ability to set up a VPN you may consider it.

Use a good and trusted anti-virus software. The market is always changing for the best free anti-virus software so you should look through reviews for the latest and greatest. Two good ones right now are AVG or Antivir.



Use a firewall. Comodo.com offers a good firewall that protects more than the standard firewall that comes with Windows along with many other free products that could be very useful.

Have good email habits. Do not open suspicious emails and do not open attachments with suspicious origins. What is suspicious? If you get an email that you were not expecting, even if its from a friend or if they ask you to do something or give them information that seems unexpected, it should be

suspect. Do not enter information in response to a request unless you initiated it. When searching for websites, and especially when looking for a software product to download, check for reviews of the site or product before downloading it. If it is suspicious, someone will probably leave a review indicating that.

Unless you know what you are doing, make sure that you have the file sharing feature disabled on your computer. This can be done by using the help menu on your computer and following the instructions.

If you have a wireless router, make sure you setup password protected encryption. If you do not, you are extremely vulnerable to eavesdropping. This may not apply if you live in a cabin in the mountains and can easily detect if someone is close enough to pick up your router signal.

When you shop online, you no longer have to use your credit card to make a payment. eBillme is a free service that lets you pay cash for online purchases. You can pay securely through your bank or, if you do not want to use a bank account, you can print out a receipt and take that into an eBillme location and pay with cash. The email address that you provide can be anonymous and no ID is required to pay. You can even get another person to go in for you and pay the cash. To find what online retailers use eBillme, there are many and the list is growing, go to their site.

DATA PRIVACY

Laptops get stolen, computers get hacked and files get compromised. Nothing is absolutely safe. Just like putting a lock on your door, you should take reasonable measures to protect your data. One very effective way to do this is to encrypt your emails or files, whether they are on your laptop or desktop and regardless of whether you are connected to the Internet at all. Use the open source Truecrypt which can be downloaded at truecrypt.org. There are several free products from Pretty Good Privacy (PGP) at pgpi.com as well. It may not be necessary to encrypt everything, but you should encrypt the most sensitive files. You may also use a program like Killdisk to completely wipe any history of what was on your computer. It can be downloaded at killdisk.com. There is also a free space wipe function with PGP which will wipe out any files that have been “deleted” but have not been written over yet. This is particularly useful to do before you sell or donate your computer.

The University of Washington has developed an interesting tool that allows users to send email messages that will vanish after a user determined expiration period passes. Although it is a prototype for research purposes, and is thus open to needing revisions, it is another arrow in your quiver of privacy tools. You can thus send a message to a friend which will not be capable of being read, by your friend or anyone else, after the time of expiration. Go to the vanish website to learn more about it and download the necessary code to operate it. vanish.cs.washington.edu.

When you save information, keep it saved on removable media, like a USB drive, rather than on your computer hard drive. There will still be temporary copies on your hard drive somewhere, but they will be slightly harder to find than if they were saved in your documents folder, as long as you keep good track of your USB drive. If you want to be fancy like one of my good friends in the cybercrimes division for the FBI then you can even get a removable hard drive and take it out every time you turn off your computer. To be extra sneaky, put another hard drive in and engage in some meaningless activity on it once in a while to make it seem like it is your regular hard drive.

SOCIAL WEBSITES

The security and integrity of social networking sites like Myspace, Facebook, Linkedin, and etc. are sketchy at best. Some privacy experts would recommend staying away from them completely, and many individuals will be willing to comply with that. There is some power that can be gained from leveraging social networking tools in business and personal life, so you may feel that the benefits outweigh the threat to privacy. If you simply follow common sense precautions when uploading any information and in your use of the site then you should be at minimal risk.

With a history of being hacked, pressure to increase their top line, government social network analysis and some functions of the sites themselves, assume that any information you provide to social networking sites will be completely unrestricted and accessible by anyone, whether you keep parts of your profile private or not. Therefore, do not provide them with any information you would not print on a T-shirt and wear to a baseball game to be seen on ESPN. You are still at risk of what your friends and acquaintances post. This is true regardless of whether you have a social networking account or not. Some employers might delve deeply into the profiles of your friends looking for photos, comments or behavior made by you or about you that could

be potentially revealing. Take whatever precautions are necessary on your social networking sites to make sure your friends do not post that kind of information.

PERSONAL ACTIVITY

PRIVACY HABIT

Making privacy a priority in your life is both the easiest and cheapest as well as the most difficult and expensive thing you can do to protect yourself. It is easy because, once the habit is developed, it is just that; a habit. You will no longer have to think about what you should be doing to guard your privacy, you will just do it. The development of the habit, on the other hand, requires attention and effort in proportion to your desired level of privacy. In this way it can be very costly to develop a habit because your attention and effort, which could be spent making money or enjoying a swim at the beach, is valuable. If making yourself vanish is a true desire of yours, whether it is to become less of a target for identity theft, reduce your profile for kidnapping purposes, avoid unnecessary litigation or privacy invasion, then the habit will not be a burden to develop and will not be a costly expenditure of time because it is truly satisfying to you. There are certain guidelines which are part of developing this habit of protecting your own privacy which will apply to everybody, regardless of the ultimate goals or motives for privacy protection.

One simple thing is to do your best to avoid the suspicion of others, both people you know and people you do not know. This is easier said than done, but is also something that follows principles of common sense. If you think that your behavior would raise suspicion in the mind of another person then you have some options. You can choose not to do it, be very discreet, or have a good reason that is generally acceptable for doing it. For example, if you follow the steps outlined in this book to set up a ghost address in a place far from your actual residence, someone who does business with you in person, where you actually reside might think it is suspicious. If part of your true motive for setting up a ghost address is to avoid being tracked by Russian spies, many people would be suspicious and think you to be a bit nutty. A response that raises less suspicion would be that you travel often or are thinking about doing a lot of traveling in the near future and therefore need to make sure that you are quickly notified of important mail.

Those who make privacy a habit and a priority in their life will find the need to balance two competing interests. On one hand, getting others to practice good privacy increases the privacy of everyone. On the other hand, challenging others to pierce your veil of privacy, invites attention and resources to meet the challenge. Sharing a desire for privacy and specific privacy practices and tools in the abstract will usually not draw unwanted attention. Even sharing some of the tools that you yourself use to protect your privacy can be useful to promote the use of those tools by others. Sharing in detail what assets and information you are protecting will to expose you to unwanted intrusion. Calibrate the level of disclosure of your privacy goals and practices with the level of trust you have in the individuals you tell.

Avoid compromising situations. There are many times and places where we know that our privacy will be challenged, such as at a border crossing or if you file a lawsuit, etc. Avoid them if possible. Change the subject of conversation if you find that it comes too close to disclosing personal information. This requires social skill because changing the conversation cold after an intrusive question raises suspicion and might make you a target more than a truthful answer might be.

If you are wealthy, or you just appear to be, realize that displaying wealth to the public makes you a target for fraud, identity theft, lawsuits and other undesirable things. Live modestly where appropriate. Partying like a rock star can be very revealing. As with all privacy issues, you can and should consciously determine how conspicuously to consume.

Know your rights. There are techniques to use when dealing with law enforcement officers that allow you to assert your rights in a respectable, non-aggressive and peaceful manner. There are many legal protections available to individuals regarding police encounters and witness testimony. Specific measures are outlined in a later section of this book. A knowledge of all of your rights is helpful to protecting those rights before you inadvertently waive them. For example, I recommend viewing the free training video BUSTED: A Citizens Guide to Police Encounters by Flex Your Rights multiple times. You can find it on the home page of HowToVanish.com.

Make sure to use your peep hole and do not answer the door when strangers knock.

Attitude and commitment will help you develop the habits you need to

vanish.

REMOVE YOUR NAME FROM DATABASES

One of the biggest threats to personal privacy in the modern era is the ability to profile an individual so well that they can be uniquely identified by the aggregation of data that is otherwise anonymous. If there are any databases that contain personal identification, such as address or phone number, pinpointing you becomes very easy. This is made possible by the extensive databases that are maintained and built by government and private entities. The less information that you have in these databases, the easier it will be for you to vanish while in plain sight.

Many of these databases will sell your information to others and make it accessible to marketers and other agencies. You can opt out of several of these kinds of databases by contacting the companies that maintain the databases and follow the instructions.

Pre-screened credit offers – Credit reporting agencies provide other companies with your personal credit information, along with lots of other personal information, so that those companies can make you offers. You can opt out of this information sharing by visiting optoutscreen.com or by calling them at 888-567-8688.

A company called Acxiom compiles and maintains detailed information on the public to sell to marketers. You can request that they refrain from selling the information on your household – email optoutus@acxiom.com (877-774-2094). You can check for inaccurate information with them for $5 at referencereport@acxiom.com (877-774-2094).

The Direct Marketing Association allows you to opt out of receiving junk mail for $1. You can do this at dmaconsumers.org/cgi/offmailing or by writing to Direct Marketing Association, PO Box 282 Carmel NY 10512. These last two are not quite free, but I'd rather give it all to your right here.

Whenever you take out a loan or deal with a bank, the company may share your information with marketers and other affiliates. You may opt out of some of this sharing of information by law. Check the privacy policy whenever you are involved in these transactions and opt out when possible. Unfortunately this often requires that you affirmatively check a box or initial at a certain point

in the loan documents to avoid the disclosure, but the opt out sections are usually fairly conspicuous and can be found with a good scan of the signing documents. Even if you opt out of sharing, the information is still within their database and will be accessible to law enforcement. This practice may also apply to countless other goods and services, although there is often no requirement by law to offer an opt out.

Keep your home address and telephone number unrelated to each other. This is done by never letting someone who has your home address also have your phone number, regardless of whether they have your real name or not. These are merely two fields in a database to an investigator and the fact that they match will increase the likelihood that they can find you. This means if you have pizza delivered to your home, do not use a phone number that is in any way connected to you. Use your temporary prepaid calling card number or unshared Google voice number or even the phone number of a friend as your phone number if you have to give it out in connection with your address.

SHOPPING

Major retail stores keep track of credit card purchases and their systems are relatively easy to hack. In addition, credit cards often share aggregated information on their customers with other affiliates. Do not use credit cards to buy something unless you are fully aware that your name and credit card billing address will be associated with that purchase. You should read the privacy policy of any credit card or other product that you use, especially if you must provide them with some personal information, to understand just what they are doing with all of the information they gather on you.

If you decide that using a credit card is acceptable for your level of privacy, there are still things that you can do when using it to enhance your privacy. Whenever you are paying for something with a credit card, when you sign the receipt, cross out the last four digits of your credit card number. Do this on both the merchant and customer copies.

Commercial copiers have a hard drive in their copy machines that store all of the photocopies made for a rather long period of time, sometimes for years. This hard drive may be legitimately reviewed or may be surreptitiously compromised. Do not photocopy sensitive documents on a public photocopier.

Lots of stores now have shoppers cards. These cards are used to collect personal infomration about the customer and keep track of all of their purchases. The stores use this information for their own marketing purposes. The information can also be used to conduct detailed profiling of the customers because so much information is gathered. Thousands of consumer databases cannot be protected from hackers when even government and bank databases are regularly hacked. If permitted by the agreement, do not provide any personal information that you would not want to give to your most mortal enemy, use someone else's card at the store, or avoid getting a shoppers card altogether.

Keep track of your credit report. Everyone has the right to receive one update per year for free of their own credit report. There are many places that you can go to access this information such as annualcreditreport.com. Other commercial data aggregators allow individuals access in order to correct inaccuracies in the information. Choicepoint (choicetrust.com) and ChexSystems (consumerdebit.com) both allow you access.

IDENTIFYING DOCUMENTS

Do not use your drivers license as identification except when asked by a traffic officer when you are driving. There is a lot of personal information on your license that you would never willingly give to a stranger, but for many people, using their drivers license as ID is simply their first inclination.

A passport is much better to use as ID because it contains far less personal information. There is no address listed and no social security number. Passports are, however, valuable to thieves and can make you more vulnerable to theft if you are seen using a passport booklet. Even better still is the credit card sized passport card Although it can not be used for international air travel, it is much easier to carry than a regular passport booklet and does not contain any history of your international travels. It also has a different number than your passport booklet. To get one you need to either mail in a passport renewal form (DS-82) if eligible, or you may need to apply in person at a post office or other passport facility. More information can be found at

travel.state.gov.

Most people want to drive so they need to get a drivers license. If possible, get your drivers license from a state that does not list your home address or SSN on the license. If you must show an address, you may be able to list your PO box or a ghost address, if legal in that state. If the application asks for "street address" you can probably use a ghost address. If it asks for a residential address, you should use your actual physical address. Ask the DMV what to do if you "just moved there" and have not established an address yet or if you are homeless. Even though you have to disclose your SSN when getting a driver license, you do not have to have it on the card. If they use your SSN as your DL#, ask to have it changed and they must comply.

When you register new software or computers, use a pseudonym. As long as you are not doing this to commit fraud there is no reason why this can not be done.

PROTECT YOURSELF FROM IDENTITY THEFT

The list of practices that make yourself less likely to be a victim of identity theft is infinite. Those specific practices are based on some fundamental principles that, when conscientiously applied, make an exhaustive list of things to do less necessary.

First is an understanding of what information is most valuable to identity thieves. The most powerful key, as most people know, is the Social Security Number. Knowledge of your SSN makes it easy to impersonate you and cause serious financial damage and privacy invasion. This should be the most heavily guarded piece of your personal information. It should only be given out if absolutely necessary.

Many times when a social security number is asked for, it is not required. Do not give it out if it is not required. This may take you convincing someone that it is not really required, even though company policy requires it, in order to receive the goods or services you want. If they insist, and if it does appear to be necessary, you should factor this disclosure into the price of the goods or services and determine if the price may be too high. It is common for some people to accidentally transpose two of the numbers of their social security number. If it is two of the last four digits, it probably will not even be detected. Do not do this intentionally because it might be illegal depending on the

situation.

The next category in order of importance includes other sensitive identifying information such as PIN numbers, bank account numbers, residential addresses, birth date, marriage date, phone number and other similar information. This should also be highly guarded and kept inside your head, rather than written on documents, as much as possible. If it is kept in a document then the document should be encrypted or coded.

TRASH

Identity thieves, private investigators and police may be able to legally search through your trash and uncover important information. Leaving your trash by the curb or in the dumpster for any period of time means that it has been "abandoned" and you do not have an expectation of privacy in that garbage. Thus the police may search it without a warrant, or others may rummage around without trespassing, stealing or violating any Fourth Amendment rights as interpreted by the Supreme Court. U You can take your trash outside right before the garbage truck picks it up from your home. You can also wait with your trash and make sure that it is loaded into the garbage truck. In some areas where you have a fireplace or are able to legally burn trash, burn whatever you can. What trash should you protect? Even a fast food receipt, product container or a newspaper can give away your lifestyle as much as a bank statement so you should destroy or monitor as much of your trash as possible, rather than simply throwing it out.

UNSOLICITED CONTACTS

If you are contacted by anyone, even if it is your bank, the pope or the president, do not disclose any personal information. Only if you are sure that you are speaking to the right representative from the entity you are contacting, and usually only if you have initiated the contact yourself, should you reveal any account numbers or identifying information. Thieves and private investigators often pose as someone else in order to illicit information from you which they will use against you. With so much personal info available about most people, it is easy for people to pretend they knew you from the young libertarians club in college.

MEDICAL IDENTITY

Just like checking your credit report regularly, you may want to look at your medical records to make sure nobody has impersonated you to receive medical care. There is even a danger that an impersonator has changed vital information about you like your surgical history. You can check your medical records at 866-692-6901 or at mib.com. Also ask your insurance company for an update on the activity under your policy.

POLICE ENCOUNTERS

Police encounters can lead to a complete loss of all privacy in the worst cases. Unfortunately, this often occurs to innocent people. Keeping certain things in mind during any police encounters and during specific scenarios can help protect you from unwanted disclosures.

IN ALL ENCOUNTERS

Always remain polite and appear cooperative. If you are belligerent and defensive, the police will be suspicious of you and escalate the intensity of their scrutiny. Also, never consent to a search if they ask. If they have to ask, they probably do not have enough evidence to search without your consent. Refusing consent is not a factor in determining whether there is sufficient evidence for a search and cannot be the basis, by itself, for the police to conduct a search. In a calm but authoritative tone say, "Officer, I do not consent to any searches."

Keep barriers between the police and your private areas, like inside your house, car or in a bag you are carrying. Step outside to speak to an officer outside of your house and close the door of the house if the police come to your home. If you are in a vehicle, roll down the window only part way unless asked to do something else by the officer. If you have a bag or briefcase, keep it closed and behind you when talking to police.

There are several exceptions to a warrant requirement to search. I will mention some of the more common ones here. If there are illegal items that the officer sees in “plain view” they may search that area, no matter where it is in your home, car or back pocket. So keep anything that could be misconstrued as evidence of illegal activity, like toy guns or cash, out of plain view at all times. There is no warrant needed to search a car if there is probable cause to believe that there is criminal activity afoot. Giving your consent is another major exception which will permit police to legally conduct a search.

If you have already consented, either explicitly or unwittingly, you may withdraw your consent at any time and the officer must then stop. You may say something like "I do not want to waste either the taxpayer's money or anymore of your time and therefore I am withdrawing my consent for you to search." If the officer has not discovered anything that would justify a search without consent then they must stop.

In the face of questioning it is usually best to be silent. Your name is usually all that you are required to give. This is far better than offering a lie to protect your privacy, even if it seems like a little white lie, it may be a serious offense. You may also tell them that you wish to speak to your lawyer before you respond to any questions. NOTE: use the term "my" lawyer as opposed to "a" lawyer. Even if you have not ever had the pleasure of ever speaking to a lawyer before, once you do they will be "your" lawyer and it implies that you are well protected legally. You may also ask to call your lawyer on a cell phone during the encounter. Both of these strategies might discourage the police from acting unconstitutionally during the encounter.

VEHICULAR STOPS

If you are stopped and you are a driver, you will be required to give license and registration to the officer. Do not give any more information than this. Do not waive your 5th amendment right to be free of incriminating yourself by answering a question from the officer. This may seem strange, but simply respond with a "why" question that would answer the officer's question to you. For example:

Officer - "Do you know why I stopped you?"

You - "Why did you stop me officer?"

(Many people respond by stating they were probably speeding or something like that. Never do this because you are admitting guilt to the officer.)

Do not say it like you are mocking the question. You might get mocked

upside the head. If you are asked a yes or no question, sometimes it is best to simply remain silent.

After any initial questions have been asked, say “Am I being detained any longer or am I free to leave?” This forces the officer to escalate the encounter or terminate it. Repeat this question every few minutes of the encounter if it seems to be taking too long.

If an officer implies or asks to search you or your vehicle state “I do not consent to any searches.” It may be best to ease the officer into that statement by saying something like, “I do not want to waste either your time or the taxpayer's money and therefore I do not consent to any searches.”

STREET ENCOUNTERS

You usually have to give your name and in some places you must show identification, but you are not required to give more than that if you are stopped by police on the street. Again, you do not have to respond to questions that you are uncomfortable with. Tell them that you wish to speak to your lawyer before you respond to any questions.

If police suspect that you might be armed they may pat down your outer clothing for weapons. Thus, avoid carrying any items that might feel like a weapon. Even if it turns out to be a squirt gun instead of a real gun, if it feels like a real gun, they may proceed to search you further.

Again the phrase “I do not consent to any searches.” is vital for not waiving your Constitutional rights.

HOME SEARCHES

Keep access to the inside of your home closed. That includes not only visually, but keep sound, smell and other things out of reach of the police. Talk to them outside with the door and windows closed behind you. Do not consent to any searches and make sure they have a warrant if they demand entry.

Some of these strategies are discussed thoroughly at flexyourrights.org and in the video BUSTED: The Citizen's Guide to Surviving Police Encounters. Watch that video over and over along with reading this section many times until you know it backwards and forwards. It will make you look like a hero in

front of your friends if you ever need it.

MAKING PERSONAL PROPERTY VANISH

KEEPING VALUABLES IN THE HOME

The remaining discussion about storing valuables has many security implications. Although privacy and security are closely linked, I do not want to confuse the issues of security with privacy. Of course the more security you have built into your house, such as locks, large fences, and gates, the more privacy you are likely to have as well. If your home is subject to a search by the police you will lose that privacy. Keeping personal property in your home or other real property is the most private of all, because you do not have to tell anyone that it is there. You can keep it in places throughout your house or even play pirate and bury it in the yard, floorboards, vases; be creative! Nobody has to know where it is if you do not tell them. You can even make an esoteric treasure map if it suits your fancy. Just make sure you do not forget where you buried those gold coins!

How To Vanish: Low Cost

In addition to free tools and techniques for vanishing, there are others that have a minimal cost in terms of money, time or effort. Most of these will still be feasible for even the poorest college student or busiest executive. In many instances the long term costs in terms of time and money will be less when following these privacy practices. I only include them in the low cost section because there is an initial expense or a change in lifestyle associated with them. Pause for a moment and take a nice, deep breath. Feel your lungs fill up until they are very full and then slowly release your breath. If all you do is read the free and low cost options and implement a few of the best ones, you will be able to feel as refreshed and secure as you do now, knowing that you are beginning to truly vanish.

LOCATION

HOME ADDRESS

Rent. Home ownership records are public information. Your name will not show up on public records in relation to the property where you live if you

are renting. In addition, it helps to rent where you can deal directly with a landlord rather than with a property manager. Property managers do not have the flexibility to make the kinds of decisions that need to be made to protect your privacy, such as avoiding a credit check, utility bills, etc. A credit check will mean disclosing your SSN to a potential landlord. You might avoid a credit check by offering to pay a higher deposit or by prepaying rent.

When you move, rent a private moving truck, like a U-haul or Ryder truck, and hire some college students to help you move rather than hire a moving company. Large movers maintain more complete databases with customer names and their old and new addresses. Your furniture might take a few more dings this way, but your privacy will remain pristine.

UTILITIES

When looking for a place to rent, find a landlord who will include the utilities as part of the rent. This is common and an offer to pay a slightly higher rent may be all that is needed to persuade them.

If you cannot find a landlord to do this, or if you still chose to buy a property, do not use your personal name to set up your utilities. You may consider using the name of a willing friend, especially if their name is on the lease or is listed as a resident of the property. Another good idea is to set up the utilities in the name of a trust or LLC, preferably the same one you might have used to buy or rent the property. You may also be able to simply withhold your name from the utility company. This will probably require a higher deposit and may raise more suspicion than you want.

COMMUNICATIONS

PHONE PRIVACY

Set up your phone service through your LLC. The benefits of an LLC are discussed later in this chapter.

Telecommunications companies maintain extensive records on your call history and Internet usage. If you make international calls, they might even be monitored by the US government. To keep your phone call records more private, use a private phone carrier like DPI (dpiteleconnect.com/public). They will accept cash and do not require you to reveal your name, there is no contract and no credit check. They may also provide Internet, long distance and other services. Their advertisements indicate that they do not need your real name to get their services, only an address.

Use pre-paid phone cards to make calls. These can be purchased in almost any grocery store or large retail stores with cash. Fool caller id and use spoofing. Spoofcard, Spooftel or Telespoof allow you to pick whatever you want to show up in the caller ID of the recipient.

You can encrypt your Internet connection along with several other services by using Identity Cloaker (howtovanish.com/IdentityCloaker) or a similar proxy server service. Identity Cloaker allows you to surf the Internet anonymously without disclosing your IP address in relation to your web activity by redirecting your traffic through their servers to do the surfing.

There are numerous call forwarding services which allow you to set up a phone number in the name of the service provider which will forward phone calls to any other number you select, without the knowledge of the caller, increasing the steps between your phone number and your identity. Jangl is one such service. Similarly, your voicemail could be forwarded to another phone or accessible by computer through private services such as J2.com. J2 requires only that you provide a valid email address. Although Google Voice offers similar services for free, most paid services do not disclose the content of your calls or messages to advertisers like Google Voice potentially does. Any service will still be subject to US law which may permit the government to engage in secret wiretapping or monitoring the numbers dialed.

CELL PHONES

Many cell phones must be used in conjunction with a specific service

provider. This is usually a contractual obligation that you assume when you purchase the phone, but there is also a technological barrier, a software lock preventing the use of that phone with other service providers, even when the contractual period has expired. Being forced to rely on a service provider limits your mobility and thus limits your ability to vanish. It is legal to override the technological barrier to using the phone with another provider, also called unlocking or jailbreaking the phone. If you are uneasy with trying to unlock your own cell phone, or if you do not want to spend the several hours that might be necessary to research the steps, download the right software, and then perform the unlocking yourself, there are services available which will help you do this. Two good ones are found at thetravelinsider.info/roadwarriorcontent/nokiaunlocking.htm or at iunlock.com. There are often local services where you can bring your phone in to have them unlock your phone for you if you feel uncomfortable sending your phone in to have it unlocked.

You can get a pre-paid cell phone from Cricket, Virgin Wireless, T-Mobile, Tracfone, DPI or even at Target and Wal Mart. Most of them allow you to pay with cash and pay for minutes as you go with cash. To enhance your privacy protection, use your pre-paid calling card to make calls on your pre-paid cell phone.

PAGERS

All cell phones store a lot of information on them and can be a hassle to keep clean of sensitive data. Your cell phone might be hacked and transmit like a microphone, even if it is switched off. Even though all the cool kids are doing it, does not mean that you have to have a cell phone. Instead of using a cell phone, or in combination with using a cell phone, you might think about using a pager. They are out of style for most people, but they do not have the GPS locating capabilities of a phone and do not have the same extensive data storage of a cell phone that can be retrieved if lost or stolen. They also continue to work more often during large scale disasters, even when cell phone networks are overloaded. When you get a page, you can select which phone you want to use to call the person back,. To avoid even further intrusions into your data history on your pager, you can develop a code with your friends and family. 1111111 call home, 2222222 call mom, 9111111, emergency, 777777 the game is starting etc. Another benefit to using a pager is that it does not record data such as photo or voice data itself, it simply receives short messages.

POSTAL PRIVACY

PO Boxes are slightly better than a home mail box because they are secured by a key. They are also good because you do not have to disclose your physical address to others in order to receive mail. Getting a PO box is relatively simple and inexpensive. You can do it online or in person but either way you must fill out a USPS 1583 form and show 2 forms of ID at the location of your PO box in order to set it up.

You may want to use a mail receiving service such as a postal annex or UPS who will receive your mail. Small mom and pop stores might even be willing to accept packages for you, especially if they are friends of yours or you are a frequent customer. Earth Class Mail is even better than a PO Box or other mail drop service because they can scan your mail so you can read the PDF from anywhere in the world and forward any particular item to your current location or instruct them to shred any piece of mail you received.

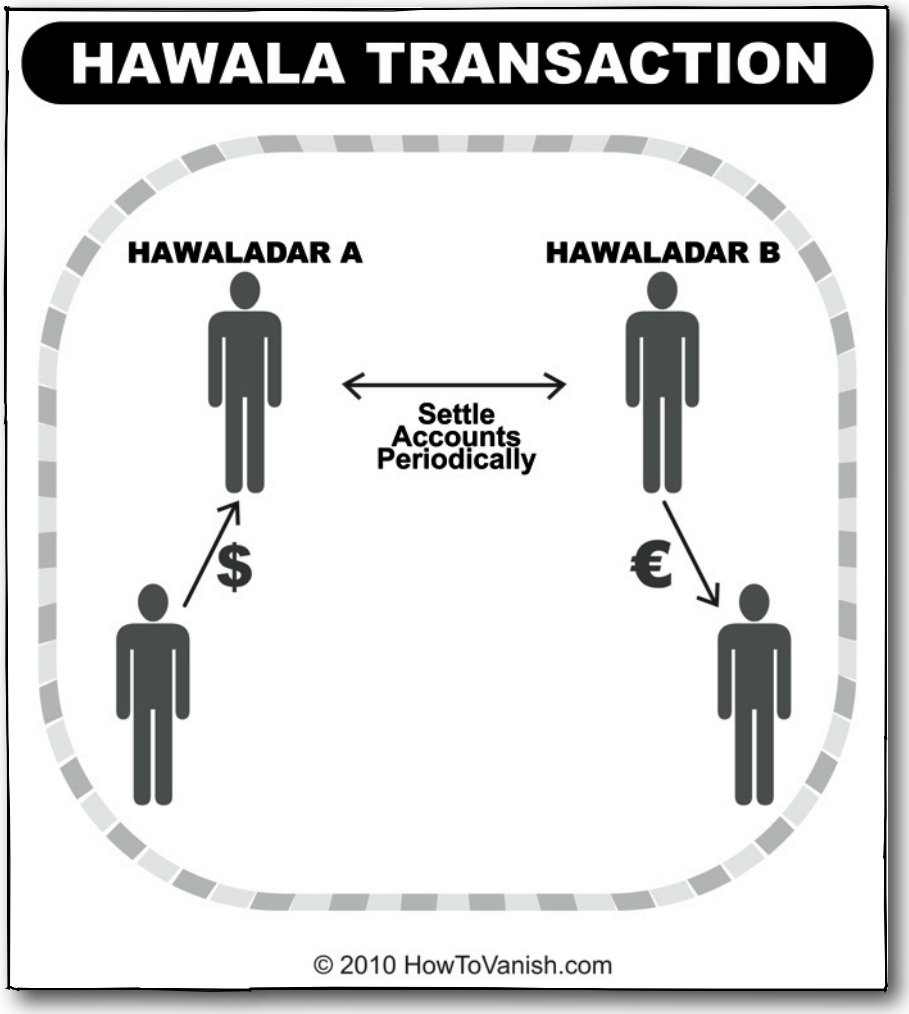
Many people regularly shop online. Doing so means that the thing you buy will have to be shipped to a physical address. Do not ever send an item to your physical address if you send it in your own name, especially if the deliveries will be made by DSL, UPS, FedEx or some other carrier. A ghost address, like Earth Class Mail, should be used in order to receive these deliveries. You may also receive packages delivered to a pseudonym to avoid many problems.

Get a foreign mail drop to receive sensitive international mail and prevent it from ever entering a US jurisdiction. A foreign mail drop will operate in a similar fashion to the domestic ones, but they are more expensive and you will have to choose your desired jurisdiction.

FINANCIAL

BANK PRIVACY

The most private way to transfer money is using the ancient principles known as hawala. This method of money transfers originated in Asia and the Middle East centuries before the modern banking system and is still widely used among many from those cultures. The most common example of how



this type of transfer works is to remit money across long distances.

Imagine if person A needs to send money to person B in another city or country. To make a transaction, person A gives money to hawaladar Y. Hawaladars are the individuals who facilitate the transaction, much like a broker. Hawaladar Y contacts hawaladar Z in that other city or country with instructions to pay out the desired amount of money when person B comes to them. Person A tells person B the necessary details and Person B then contacts Hawaladar Z and gets the money that was paid by person A to hawaladar Y minus a small fee. The hawaladars settle their accounts of several transactions with each other at a later date.

Hawala transactions are more efficient than western style transactions and there are almost no instances of fraud because the system is largely based on

strong relationships of trust between family or long time friends. Hawala is under strong criticism in the West as being facilitative of terrorism and money laundering even though it is overwhelmingly used for legitimate transfers. Many places have created laws that heavily regulate or make some aspects of hawala illegal. For this reason hawaladars are hard to find unless you make transfers with your own network of friends, family and business associates. If you do use hawala principles, they are among the best ways to transfer money anonymously.

Another strategy is to set up a bank account in the name of a business you own rather than in your own personal name. You will probably still have to associate your name with the account, such as making yourself an authorized person on the account, in order to conduct business, but having the ownership of the account in the name of a business will provide an extra layer of privacy protection.

TRANSACTIONS

Cash is not totally anonymous. Every bill printed has a serial number. If someone is interested in finding out your cash spending habits, with some resources they can acquire the serial numbers of the bills that you are given and where those bills were spent and when. One way to avoid this is to pay for everything with quarters, dimes and nickels. I do not recommend this approach.

Gold and silver, in the form of coins, bullion and jewelry, is not identified by serial number. It is truly anonymous and sovereign wealth. It is not free, however, because there is some cost to using coins in daily transactions in the US. Unlike much of the world where gold is the equivalent of currency and can be exchanged for goods and services rather easily, US citizens do not universally recognize gold as money or currency. Thus there is some cost to finding individuals willing to deal in gold as well as the a cost for the premium of a gold coin rather than bullion. Even though a Goldmoney account is free to set up, if you are going to hold any gold or silver ounces, there is a storage fee and there is a cost for every wire transfer to deposit or withdraw funds from your account. There is also a small transaction fee when you transfer gold, silver or platinum to another holding.

The Internet provides many options for purchasing products electronically, without setting foot out of your house or ever dealing face to face with another

person. But this kind of transaction cannot be done with traditional cash to keep it anonymous. To make Internet transactions vanish in connection with you, use prepaid gift cards.

Gift cards can be used without disclosing any SSN, credit history, and many other pieces of personal information. Although some terms of use say they require online registration of the card if you want to use them to make online purchases, the registration usually asks for a name and an address, not a SSN. Often, the only registration required will be at the point of sale where you will need to provide the name on the card and a billing address. The name on

the card I have used is simply "gift," which is what is printed where a name would normally be found on a credit or debit card, and the address I provide is the ghost address which I use to receive deliveries. If permitted by the user agreement, you may be able to have a friend receive shipments in their name.

Purchase a gift card such as a Visa or Mastercard at a local grocery store or convenience store using cash only. They are usually with the prepaid phone cards.. They work as an anonymous card at most stores where a regular debit card is accepted, without having a related bank account. You can also log onto an online retailer, do your shopping and proceed to checkout. Enter the gift card info like a credit card. There will probably be an expiration date on the anonymous card as if it were a credit card. Ship the item to your alternate or ghost address (not your home address) and ship it to the name that you use to receive mail at that address.

There are some significant downsides to using gift cards like a $200 maximum. Some vendors will be willing to split the payment over several different cards at once, but others will not. The small fees for using the cards can become significant if you are using them often. Gift cards can usually only be used inside the country of purchase.

IRS

The IRS has significant legal authority to invade privacy. Vast reporting requirements of common economic activity invades your privacy. Compliance with all tax laws is the best way to avoid further invasion via an audit. It will help you sleep well at night too. The laws regarding taxation and disclosures change so frequently that compliance is difficult without the assistance of tax professionals. You should always seek the assistance of accountants and attorneys when dealing with tax issues that affect your individual situation. The scope of this book is about privacy and not about illegally evading or legally avoiding tax liability.

ELECTRONIC

PC

Get an anonymous email address. You can send anonymous emails from some web sites. With Hushmail you can have an anonymous email account that does not keep track of your IP address like other anonymous emails. The paid premium service is much more usable than the free service, even though it is not more private.

Spyware, viruses and other threats to privacy from online activity is a topic thoroughly covered by many others. Get the appropriate anti-virus, anti-spyware software and keep it updated. Norton and McAfee products are well known as being good, trusted, paid services which usually offer important improvements over the free antivirus and anti spyware versions.

Use a Privacy Screen on your laptop if you use it in public places. This prevents people from looking over your shoulder and seeing what is on your screen. These can be found at most computer or office supply stores.

Computer displays emit Van Eck emissions which can be monitored from hundreds of yards away. These emissions reveal everything that you type or see on your computer screen. To avoid exposing yourself in this way, use a laptop rather than a desktop computer. Laptops reduce, but do not eliminate, these emissions.

To avoid linking your physical location with your Internet usage, there are various ways to get wireless Internet access. Satellite access has been available for several years and satellite providers can be contacted to get access. You can also cable or tether your cellular phone to your computer to get Internet service through your cell phone. Wireless Internet Service Providers like Verizon or AT&T have plug in cards for laptops which show your general location but not your exact address. Some laptops have this service built in.

Freenet is a powerful open source program which allows you to anonymously publish and download information without fear of censorship. Communication over Freenet is encrypted so it is very difficult and expensive to determine who the users are and the content of their communications. Darknet is an advanced tool available with Freenet that allows you to create an invitation only network. This allows you to limit access to the network to only trusted individuals and its existence is extremely difficult to even detect, let alone decipher. Freenet is totally free but it does require some time to learn how to use it.

PERSONAL ACTIVITIES

IDENTITY THEFT

A small expenditure on a cross cut paper shredder is another way to protect your trash privacy. Shred any document that you discard. Rummagers may still put together a profile of you based on the product containers you discard and other things, but your more sensitive personal information which you shred will not likely be recoverable.

FreeCreditReport.com, along with many banks and credit card companies, offer services which will update you when important changes are made to your account or credit report. This can help catch suspicious activity quickly.

MEDICAL PRIVACY

The most important thing you can do to keep your medical history private is to pay cash for medical services, if feasible. There are many doctors who will accept cash. You may even be able to convince your local doctor to accept cash rather than insurance because he will be paid immediately and not have to deal with all of the paperwork that comes with insurance payment systems. You still can, and should, get insurance for catastrophic illnesses or injuries, but it is best to avoid using insurance to pay for every check up or refill of prescription eye drops.

If you prefer to use insurance to cover more than just the catastrophic events, look for a doctor that is a non-covered entity. This means that the insurance paperwork that the doctor submits is in actual paper form, they do not submit stuff electronically. This makes it more costly in time and money to enter and maintain comprehensive information of your insurance activity into medical databases. You can get a high deductible insurance plan, which are less scrutinized than a low deductible plan. Also, avoid using any personal health record option because the insurance company may share that information with anyone they choose.

There has been some recent discussions about storing medical records on cell phones so that they will be portable with the person. This can be dangerous because the information will be much more accessible and difficult to keep private. If given the option, I would recommend not storing any

medical information on your cell phone.

Simply asking your doctor about keeping some things as private as possible by not sharing your information can be helpful. You can further enhance your medical privacy by asking your doctor for any professional samples of prescription medicines that you might take. If your doctor can provide them, you will avoid having to go to a pharmacy and disclosing your medical information yet again to the pharmacist.

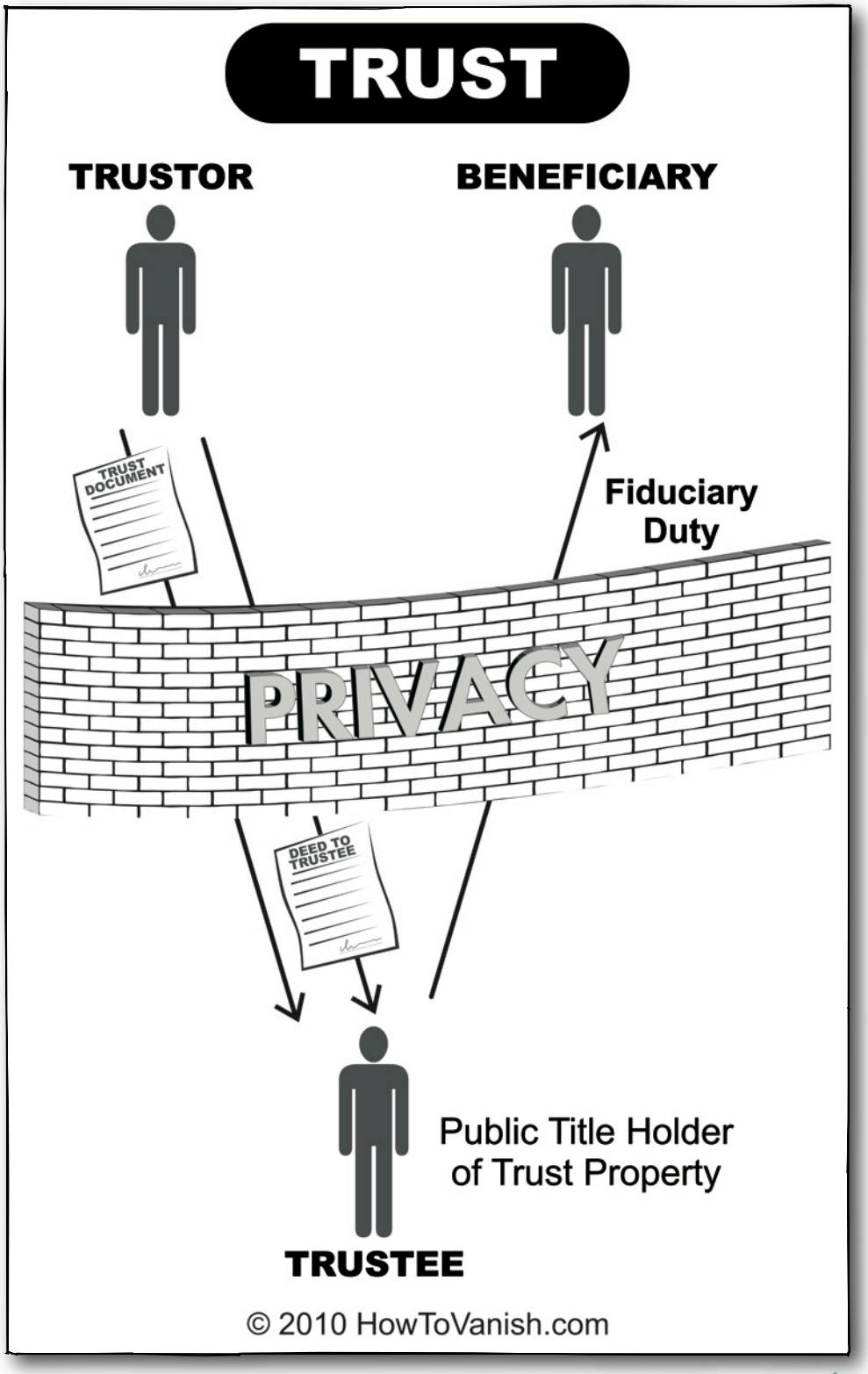
You can always choose to have medical treatment in another country where you do not have to disclose the same amount of information to get medical treatment. The cost of travel may be high, but the cost of treatment might be significantly lower. Prescriptions may also be available in those countries, but you must have the proper paperwork to bring those prescriptions back into the US legally.

LEGAL PROTECTION: DOCUMENTS

There are several documents which you should have prepared for you by a competent attorney which provide privacy for your assets and the assets of your family. These include the following:

Living Trust: This is similar to a will. It will distribute your property at your death to those whom you choose. It has many privacy advantages over a will. First, it can be drafted to distribute your property not only at death, but if you are incapacitated. If you are unfortunately hit by a bus and in a coma for 10 years, the beneficiaries are not left without the ability to use those assets for their maintenance and support. Your estate will avoid probate if distributed under a proper living trust. If you distribute your assets under a will at death, the will must go through the probate process. In probate, the courts and public will have access to the contents of your will and all of the information, including what property is disposed of in the will. In many situations the executor of the will will have the power to determine what assets are sold to satisfy outstanding debts. With a trust, the assets may be distributed by the trustee without such disclosure.

Medical Power of Attorney: If the unfortunate bus incident should occur, a MPA will allow another person to make important medical decisions for you if you are unable. This allows you to maintain as much medical privacy as possible should you find yourself in this situation. This can be very valuable


TRUST
TRUSTOR
BENEFICIARY
TRUST DOCUMENT
Fiduciary Duty
PRIVACY
DEED TO TRUSTEE
Public Title Holder of Trust Property
TRUSTEE
© 2010 HowToVanish.com

given the penchant for the US government to make public the private medical details of an individual if it is in their political interest to do so.

Living Will: A living will is very much like a Medical Power of Attorney except that it is more specific about how future medical care is to be handled, rather than allowing the agent complete freedom to determine the course of medical care. It is generally not effective until you are severely incapacitated. This document can be effected with a Medical Power of Attorney or without it, and it is another good way to maintain your medical privacy.

Durable Power of Attorney: After the bus incident, this will allow another person to make financial and business decisions in your place. Having a DPA will allow you to maintain your business and financial affairs functioning as if you were able to direct them. Much flexibility is permitted in drafting this document. You can tailor it to fit your needs including what powers you give, what specific transactions or types of transactions will be authorized and when the DPA actually goes into effect. With all of these documents, Living Trusts, MPAs, Living Wills and DPAs, choose a person to administer them who understands your desire for privacy and protection and who is willing to make the decisions that best align with your wishes.

LEGAL PROTECTION: SIGNATURES

You can instruct someone else to sign for you and you may sign for someone else with their permission. For example, if you receive a package in the name of your friend Mike Smith at your home, you can sign it Mike Smith if Mike Smith has given you permission. It is probably best if you can replicate Mike Smith's signature well, but there is little chance that the two signatures will be compared. If you get a durable power of attorney with this person, you may act in their behalf on accounts, and they can act on your behalf. That way you can set up a separate account in their name and, with their permission and

their signature, conduct all business under the account. The source of the funds in the account is irrelevant as long as it is not from illegal activity. The same is true of checks and any other document that needs a signature. Therefore you can have your name signed without you even appearing in person, or you can do things in the name of another person, without having your true identity revealed. When working with a friend, you may want to work together to develop illegible signatures that you use in such situations if you are worried about comparison of signatures.

If the identity of a member of an LLC must be disclosed, you may use a nominee as the sole member. A nominee can usually be any person with capacity (eg: eighteen years old or more and mentally competent) but it is best to select someone you can trust. The IRS will not accept the nominee when getting a tax ID number, so there are some limitations which apply.

LEGAL PROCEEDINGS

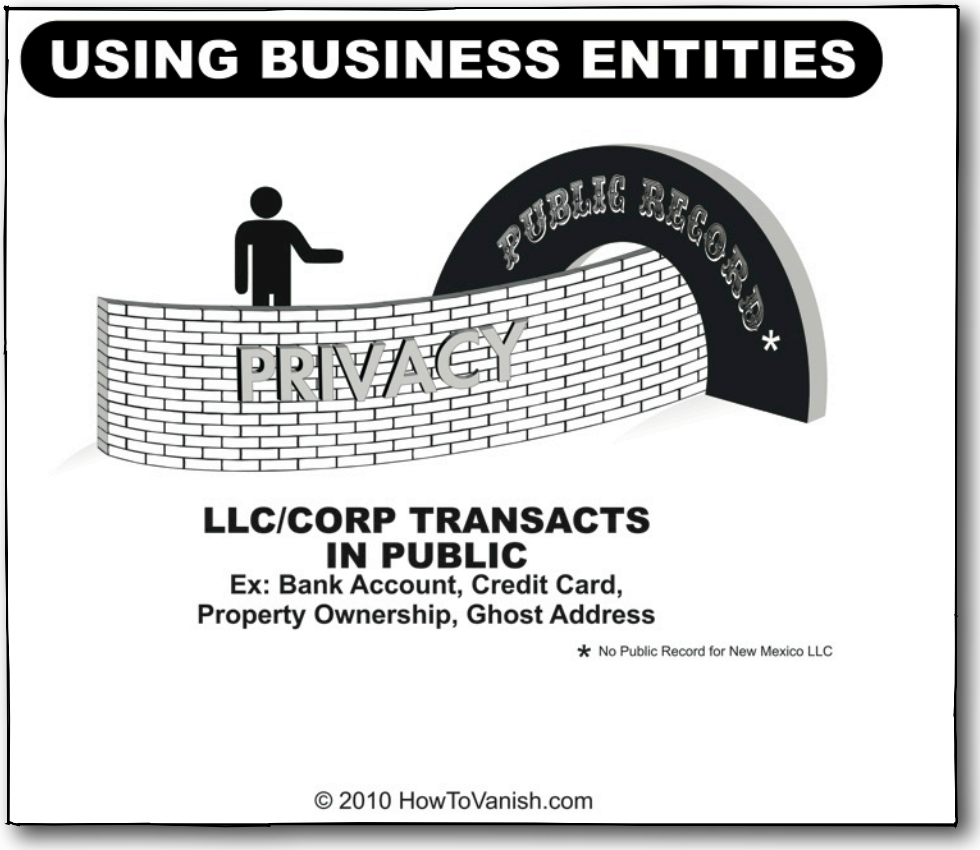
Proceedings in court open you up to many kinds of privacy invasion, no matter what the legal proceeding is. You may be subject to invasive discovery procedures like depositions or interrogatories. At the very least, court documents are open to the public and so the information contained in those documents is available to anyone.

There are significant privacy benefits to resolving disputes in arbitration or mediation. These proceedings can be kept private and the contents of documents are not available to the public. You are giving up the right to be heard by a jury if you resolve a dispute in this manner, so it is not free, but monetarily it is also usually less expensive, quicker and there are more broad resolutions available with these types of dispute resolution. You can take advantage of mediation by including mediation clauses in your contracts or, if you are already involved in litigation, by asking your lawyer to contact the other party's lawyer about voluntary mediation of the dispute.

If you have been involved in a public court proceeding, ask your attorney to have the record sealed to protect your privacy. If this is not possible, ask to have the record redacted to remove SSNs and other private data from public view. It is usually the responsibility of a party to the proceeding to request that this information be redacted.

Preventing legal proceedings being brought against you is an extremely

effective way to protect your privacy. A good general principle is to treat other people the way you wish to be treated. If you act with integrity, honor and respect, do not lie, cheat, steal or kill and avoid other nefarious behavior or situations of moral turpitude then it is highly unlikely that you will get entangled in legal proceedings. Even honest people get sued. In that case you may wish to use all reasonable methods to settle out of court with non-



disclosure agreements. But remember, the enforcement of one's legal rights is never a moral wrong and may often be a moral duty. Avoid squabbles if you can and if you choose to fight, pick your battles extremely carefully.

BUSINESS OWNERSHIP

Owning your own business and being your own boss permits you to avoid the unsavory disclosures required of employees and permits far more control and personal freedom than being an employee. Even applying for a job as an employee can subject you to credit checks, background checks, drug testing and other invasions of your privacy. Not being an employee means that you can avoid these intrusions more easily.

It is essential to your privacy that you conduct your personal business under a legally recognized entity, such as an LLC or Corporation, rather than in your own name as a sole proprietor. This not only protects your privacy but as long as you comply with applicable laws and formalities then the legal entity will help protect your personal assets via limited liability.

Operating under a business entity will also permit you to own assets in the name of the entity, discussed later in this chapter, and allows you to rent property, pay utilities, or open a bank account and even credit cards in the name of the entity rather than your own personal name. Even though in many cases you will still have to provide your own name and information to the bank or other financial institutions, those who you deal with on a daily basis for regular transactions will only have access to your business name and business information rather than your own personal information.

Choosing which business entity to form and how to structure it, as well as being compliant with applicable laws depends on the circumstances of each individual. There is no one-size-fits-all approach to forming an entity. Although an LLC generally provides more privacy, that form may not be suitable for the kind of business that you operate. Advice from a competent attorney and using an attorney to form your business entity is critical to achieving the desired privacy and liability protection. Failure to do so properly can lead to 'piercing of the veil' which is a failure of your entity to do anything to protect you personally or financially.

SPY TOOLS

The market is full of spy tools. Some of them can be elaborate bugs or listening devices, some are as simple as a pair of binoculars. Most of the intrusion that results from them can either be detected or defeated easily.

Take for example a laser audio surveillance device. Window panes vibrate to the sound of conversations inside. A laser pointed at a window pane can send the signal back to a receiver to listen in on those conversations. This device can cost up to $42,000, so it is probably only being used by professionals with deep pockets if it is used at all.

All it takes to defeat the use of this device is to have frosted glass in the windowpanes or, simply play music in the room at a louder volume than the

sensitive conversation. This technique will also stop most devices used to listen through walls which are nothing more than very sensitive microphones. If you are not a music lover, you can put the speakers up against the window panes, floorboards, walls or ceiling so that the vibrations from the speakers are transmitted directly into the building material. This reduces the volume necessary to overpower the devices from hearing your conversation.

Similar solutions are probably the best for any other of the spy devices available. Most spy tools will be defeated by a low tech, inexpensive measure that takes little more than awareness and care to make effective. There are lots of products, some good, some terrible, which prevent being spied on. For example, telephone systems in the US have built in wiretapping capabilities, made famous in the eavesdropping of international calls by the US government over the past few years. No bug detector can detect this. On the other hand, a privacy screen for your laptop is a great way to keep others from seeing your laptop screen without being extremely obvious about it.

CHOICE OF RESIDENCE

Avoid living in a very small town. In a place where everyone knows everyone, it will be very difficult to remain anonymous to your neighbors, despite your best efforts. If you live in a rural setting where it is uncommon to have contact with anyone, even if you are not avoiding it, it becomes easier to remain private. Otherwise, crowds offer the best anonymity.

MAKING PERSONAL PROPERTY VANISH

SAFETY DEPOSIT BOXES

Safety deposit boxes can be rented from a bank. They are not very safe at all and there is a ripe history of abuse and government confiscation. Whatever you do, do not store currency in them. If you want to insure the items stored, you have to have an appraisal of the items and list them as valuable items on a schedule of assets. This list is subject to subpoena in a judgment and therefore provides little privacy.

You must also disclose your SSN to the bank in order to comply with banking laws. Failure to do so could lead to a Suspicious Activity Report.

VEHICLE OWNERSHIP

Using an LLC to hold assets is a good way to separate those asset from your name. A New Mexico LLC can be created without disclosing the name of any members. For purposes of keeping asset ownership private, it is best to keep only one major asset per LLC.

Setting up an LLC for the sole purpose of owning your car has many privacy benefits. The car is not registered in your name and therefore is not directly traced to you. New Mexico may be the most beneficial to maintaining the privacy of the owner because the managers or members (owners) of the LLC do not have to be disclosed to the state or anyone else. In many other states the managers or members are either known to the state or are a matter of public record. There are some states where you give up the right to refuse a police search of the vehicle if it is owned by a business entity rather than yourself.

Make sure you pay cash and buy the car from a private seller, not from a dealership or used car lot. When you register it at the DMV then register it in the name of the LLC.

There are also advantages in getting insurance because you do not have to link the location of the car or your physical address to yourself on the application. The same can be done for renters or homeowners insurance. Making inquiries and claims against your insurance is stored in a database and is used to determine future insurability. If each vehicle and property is held by a different LLC, making a claim on one will not show up on the record of the other entities.

Transferring the asset held by an LLC is also beneficial to privacy. Rather than transfer title to the asset, the ownership of the LLC passes. Thus you do not have to go to the DMV to register a car under a new name, because it was the LLC that was transferred, not the car. Again, a New Mexico LLC is ideal for this purpose because you can transfer ownership anonymously.

Many people wonder about the tax implications of having one or more LLC's used to hold assets. Generally, the LLC will be treated as a 'flow through' entity and because you are the sole owner of the LLC, any income or losses incurred as a result of operations would generally be included on your

own personal tax return. You should fill out and submit schedule C with your personal tax return for each LLC that you own which has an income or loss. If there is no income or loss in the year, or if the income or loss is an immaterial amount, like $50, then you likely do not need to report it at all.

How To Vanish: Moderate Cost

The tools and practices discussed in this chapter are more costly or time consuming than those in the previous chapters. Still, most people will be able to afford the time and money to do a few of these recommendations that they deem to be of the most value to them. Sit up, stretch out your spine and prepare yourself, because you are about to learn how to implement some of the most powerful tools that the law provides for protecting your privacy.

LOCATION

HOME ADDRESS

Some people prefer to own their home rather than rent. It provides a greater sense of stability and you have more freedom regarding decisions about the property. In order to achieve privacy in home ownership, the property should be owned in trust or by an LLC. It is a good idea to name the trust or LLC something that does not betray your involvement. If your name is

Barack Obama, for example, and you establish the Barack Obama Family Trust to purchase a home, the public ownership records will show the name of the trust which gives away Barack Obama's involvement. A better choice might be the 123 Main St. Trust. The details of establishing a trust or LLC is explained elsewhere in this book.

Historical records of home ownership are also public. This means that even if you want to remain in your current house and transfer the title to a trust or LLC there is still a record of your prior ownership and a record of the transfer. It is best to buy a new house under the name of a new trust rather than just transferring your current house from your name to a trust, but it can still be helpful. Some people might assume that you no longer own the property, especially if the name of the trust or LLC obscures your involvement.

There is also some benefit to renting a property in the name of a trust or LLC. Rental records are not public information like property ownership records, but there is a lower risk of your landlord disclosing some piece of sensitive information if you are renting in the name of a trust or LLC rather than your own name.

Remove your name from voter registration records. Not all states offer the option of removing some of your private data from shared voter information. Avoid registering to vote in those states. Other states offer varying options for removal of information from voter lists. Contact your local elections office to find out what options are available in your area and remove as much sensitive information as possible or simply remove your records completely. You will not be able to vote if you do this but you will not appear on the list of registered voters along with your sensitive information like phone number or address.

PO BOX

If you are opening a PO Box, rather than include your permanent address, you may rent a small apartment for the month when you open the PO box and

list it as your physical address. Then move without giving the post office a forwarding address.

You could also take over a PO Box from a friend. You must be sure that the post office will deliver your mail to that box so be sure to have mail delivered to you in a manner that you can receive it. I have rarely had a problem with receiving mail at a new address, even if the name on the mail has never been associated with that address before. PO boxes are different and require you to show identification for use of the box so you might want to have mail delivered in your friend's name, or another nominee willing to show identification, to receive your mail. Pay the fees with a money order or pay your friend directly and have them continue to pay the fees for maintaining the PO box.

COMMERCIAL OFFICE SPACE

Many office buildings allow companies to establish a business identity. This allows you to maintain the appearance of a location, receive all of your business, and possibly personal, mail and meet with clients in a professional setting, while still keeping your permanent work location and home address private. You may be able to rent access to a conference room of their building, in many cases they will include your company name in the building directory. They may also have a secretary or mail room that receives the mail and will receive your mail and packages for you.

Some office buildings might be willing to rent out a broom closet to your company and allow you to receive mail there. This will probably require you to exercise your persuasive abilities to convince the owner or manager of the property to allow the arrangement since it is not common. You will want to have a suite number included in case anyone stops by to check it out. If the door is locked they will probably never realize that your office space is not big enough to even hold a single desk. This also lets you receive mail without ever disclosing the actual location of your residence or even disclosing your identity to a receptionist.

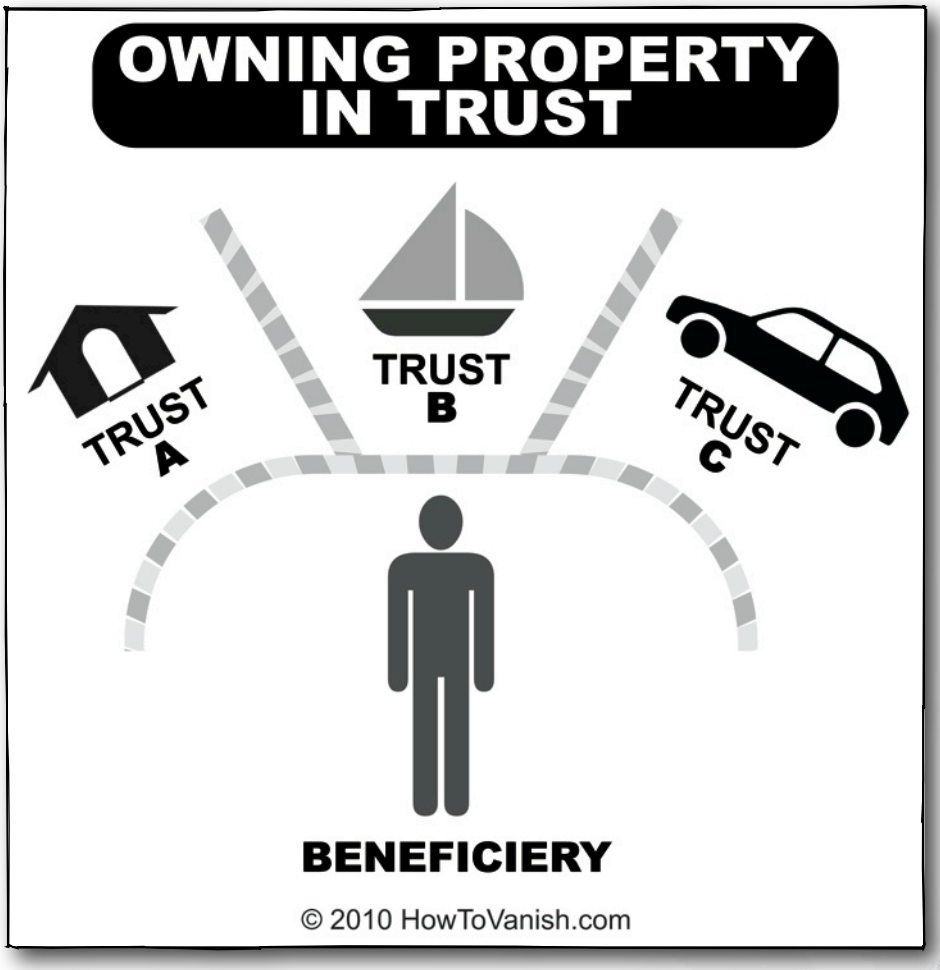
LAND OWNERSHIP

Real estate ownership records are public. Owning the property in trust, as I have already described, keeps your name out of public records. This is applicable to all types of real estate including everything from a lease on an

apartment to ownership of a large commercial building and everything in between.

Here is how the legal relationship of a trust works. The trustee is the person or entity of public record that holds title to the land. The trustee has a legal duty, or fiduciary duty, to act in the best interest of the beneficiary which receives all benefits of ownership. The trustee is bound to follow the instructions of the beneficiary, as long as they don't violate the terms of the trust. The terms can include confidentiality.

Forming an LLC to act as the public trustee creates another hurdle to piercing your privacy, especially if you name it well. The beneficiary, you, will remain anonymous because the trust document is not publicly recorded and the trustee has a duty not to reveal your identity. If you use a New Mexico LLC, your involvement will remain confidential.



In order to form this trust relationship to own land you will need an attorney to help you execute two documents. First, the Land Trust Agreement. This establishes the trustee, beneficiary relationship and defines and limits what is to be done by each. Next, the deed to trustee is executed which transfers the property to the trustee.

There are also significant reductions to personal liability if you hold property in trust as a beneficiary. Owning a different asset with all different New Mexico LLC trustees makes it very difficult for potential plaintiffs to assess your financial position, let alone encumber the assets of other trusts. Knowing that you have significant assets makes any good plaintiff's attorney salivate. Even using LLCs from other states adds an extra step to discovering true ownership of assets and can help reduce unwarranted litigation.

If you want to use an individual as a trustee instead of an entity, avoid using family members or anyone who shares your last name or has lived with you at any time in the past as a trustee. I would recommend using an attorney as the trustee of your trust. Even though any adult with capacity can be a trustee, an attorney is usually a good choice because they are able to explain the legal relationship to banks and creditors etc. Plus they have to follow a higher standard of ethical rules when managing the trust property than a non-attorney, and most lawyers are a lot of fun to be around.

COMMUNICATIONS

PHONE PRIVACY

To make the content of your phone conversations vanish, you might consider phone encryption. A company like Endoacustica sells encryption for both cell phones and land lines. When both ends of a conversation are using an encrypted phone, the conversation is very secure. If only one phone is using encryption, the conversation might be very easily intercepted at the unencrypted end.

There are very strict laws regarding the use of encryption in the US. All commercial encryption in the US must reveal their key to the US government. Many of the most secure encryption may only be used outside of the US.

POSTAL PRIVACY

If you qualify for and file a protective order with the post office, they will not release your postal information to anyone. This requires the advice of an attorney and is not likely to be applicable to most people.

FINANCIAL

TRANSACTIONS

If you are a business owner it is most private to do all of the work yourself. If you need help, it is better to hire independent contractors rather than employees. The regulations that attend hiring employees don't make it easy to avoid scrutiny from some governmental agencies.

OFFSHORE VARIABLE ANNUITIES

Variable annuities are investments through an insurance company which have several tax and legal benefits to their ownership. Although there are other vehicles, such as an IRA, that offer more benefits, a variable annuity might be considered after you have made the maximum contribution to those other assets. This is not meant in any way to serve as tax or investment advice. You should always consult with tax and investment professionals to verify compliance with applicable laws in this area. Using an offshore variable annuity allows you to take advantage of the privacy that these arrangements offer. The difference between a domestic and offshore variable annuity is simply where it is found and what law applies. An offshore variable annuity will probably be more expensive because it is offshore, but it will not be subject to the same domestic legal requirements. Offshore annuities are not subject to US qualified intermediary requirements , the "know your customer" rules, that even offshore banks are subject to.

Rather than get into the exciting details of how a variable annuity works and its tax and other benefits, I will focus on the privacy benefits of an offshore variable annuity. The first thing to consider is the jurisdiction where you will enter into an offshore annuity contract. Be sure to select a jurisdiction that will honor the privacy of the agreement. A good quality jurisdiction will be one in which the release of private information on the contract, even under authority of a US court order, is not permitted. Some suggested jurisdictions

are the Isle of Man, Lichtenstein, Switzerland or Panama. Also be sure that the issuer of your annuity, likely an insurance company, does not have US affiliates over which US courts have jurisdiction so that a US court attempt at compulsion has little persuasive power over the issuer.

If there are no contacts between the issuer of your annuity and a location where US law applies, then those assets are not subject to inspection by US courts or the IRS and not subject to attachment by a judgment in the US. You should always report all income from your offshore annuity. Even where there has been difficulty historically for the US to gather financial records of US citizens, the US is exerting new influence over foreign powers to compel disclosure of accounts of US citizens abroad. An OVA still might reduce your risk of an audit which is a threat to your privacy.

Adding another level of protection is to make the owner of the annuity a trust. In this way the trustee can withhold disbursements to the beneficiary for any legal reason depending on the trust agreement. The payment can be made for the benefit of the beneficiary rather than directly to the beneficiary.

These annuities are generally far less expensive than an offshore trust but you usually must travel to the jurisdiction in order to execute the agreement.

OFFSHORE BANKING

Many foreign countries have much stricter bank secrecy laws which protect a depositor from disclosure of their information by the bank. In Switzerland, bank secrecy is protected by their constitution. Unfortunately, most Swiss banks are no longer accepting deposits from US customers. If you are a US citizen, getting citizenship in another country as outlined later in this book might be a good option in order to take advantage of the constitutional privacy protection

offered by Swiss law. Even if there are no bank secrecy laws in the jurisdiction that you select, the simple fact that your bank is in a foreign jurisdiction adds a level of privacy to your bank account.

There are also many reporting requirements that the US has regarding offshore accounts. You must declare the aggregate amount of your foreign accounts on the FBAR form if they exceed $10,000 at any time during the tax year. Failure to do so can lead to stiff penalties. Also, if you transfer your money from a US bank to your foreign bank account, there will be a record of the transfer and you might have to explain what happened to that money.

To avoid wiring money directly to your foreign bank, many foreign banks will have a domestic affiliate who can then deposit your money in the foreign account for you. There will still be a record of this transaction. You can increase the privacy of transactions with the foreign bank by traveling there in person and conducting your business.

The USA PATRIOT Act allows the US to confiscate the assets of US citizens held in foreign banks. Foreign countries are also under severe pressure by the US to make sure that the privacy laws that protect the bank secrecy of foreign citizens do not apply to US citizens in those countries.

Take reasonable steps in order to avoid probate in a foreign country upon your death if you have any offshore accounts or assets. The stricter privacy laws in some other countries may prevent the bank from informing your family of your account, even if the bank is aware of your death, and so it is important to inform someone in your family or an attorney of the existence of the account and their interest in it. You may want to designate a beneficiary as soon as possible upon opening the account.

Numbered accounts may be available in which business is conducted with the number and password rather than in your own name. Numbered accounts are not totally anonymous accounts because your personal information will still be disclosed to the bank at some level. Although this is not a bullet proof method to maintain privacy, it keeps your identity from being exposed through day to day transactions. Truly anonymous accounts are still available in some very politically unstable regions of the world and so are very risky.

You can use a debit card issued by a foreign bank to withdraw cash and make purchases from your offshore bank account. The transactions aren't

subject to warrantless searches by police and the data probably won't be sold to marketers.

OFFSHORE INVESTING

Once you have an offshore bank, you may be able to instruct the bank to make purchases of foreign securities for you. These purchases can be made in the name of the bank and so will not bear your name and they will not be subject to SEC regulations. If you have an offshore bank purchase securities for you, avoid having them purchase from US markets. Qualified intermediary agreements force foreign banks who purchase US stocks to identify the individual they are purchasing for or void the sale. Often you are required to travel to a foreign country to issue any instructions regarding purchases or sales on your account. If you are issuing directions to your offshore bank from the US, you may be one of the individuals that must be identified or otherwise prohibited from trading in those markets.

There are fewer restrictions against US individuals purchasing bonds in a foreign bond market. This allows you more easily to direct your offshore bank to purchase or sell your bonds without having to travel outside of the US to issue the instruction.

Some investments do not easily trigger the reporting requirements of the FBAR. These include foreign real estate, warehouse arrangements for storage of allocated commodities such as gold and oil, or vaulting valuable items in other countries. These investments can be purchased and held in greater secrecy than the other instruments discussed here. Also, using trusts or LLCs to own foreign property increases the level of privacy of that foreign property.

A domestic IRA can be used to fund offshore investments which will be less visible than investments in the US. You should discuss this option with the person managing your IRA.

OFFSHORE LIFE INSURANCE

Similar to offshore variable annuities, offshore life insurance provides several benefits, including enhanced privacy of your assets. An individual who is not making payments on the policy, and who will probably outlive the payer, can be insured and have access to those funds. The insured can also take out a tax free loan against the policy and use those funds for the benefit of the

payer without the payer showing the policy as an asset. As with any investment strategy, there will be important tax and legal requirements pertinent to every unique situation, so the advice of competent tax and legal professionals should be sought.

PRIVATE INVESTMENTS

Trading precious metals is possible even without triggering the reporting requirements that banks usually have for the same size of transaction. Although there are still some reporting requirements, large amounts of coins and bars can be traded without any reports being filed. It is also relatively easy to find a coin dealer that deals in regular coins, or you can attend coin shows or deal cautiously on Craigslist.

Collectible items are another way to store value. These items can include anything from collectible coins to diamonds, artwork or vintage guitars.

BORROWING MONEY

Any time you borrow money you are compromising your privacy. Your creditors have a claim against your property and thus have a right to some of your private information. Avoid borrowing whenever possible in your own personal name. There is less risk to your personal privacy if you borrow in the name of your LLC, although many times you will have to disclose personal information anyway when your LLC is borrowing money.

PERSONAL ACTIVITIES

MARRIAGE

Getting married is inviting another person into your life who will have access to many of the most intimate details of your life. It is inherently reducing the privacy of both individuals. My recommendation of whether or not to get married is not likely to change the attitudes and beliefs towards marriage that people have. There are certain things to keep in mind if and when someone gets married to maintain as much privacy as possible. Not necessarily from your spouse, but from others outside of the relationship.

The laws of states differ, but one good way to keep you and your assets

private is by prenuptual agreement. This is not to keep assets hidden from your spouse, but to keep creditors of one spouse from reaching the separate assets of the other spouse after marriage and for other reasons. A prenuptual agreement must be very carefully drafted and should only be done by a competent attorney. After marriage, it is also important to keep your separate property separate. Don't commingle funds or put your spouse's name on the separate account for any assets or debts that you want to remain separate from the other spouse.

Divorce is actually the greatest threat to privacy posed by marriage. When a marriage ends in divorce there are adverse persons with competing interests that know the intimate details of each other's life. There are some measures to take in order to limit the publicity of the divorce. You may either choose a no fault divorce, where there is no evidence presented of behaviors of the divorcing spouses, or you may choose to have a private divorce. A private divorce is performed by an arbitrator or private judge and only the final decree is made public. This must be consented to by both spouses which may be difficult at the time of divorce but it is a good option if possible. You can look in local legal publications or the Internet for such services. Because the likelihood of agreeing on the color of the sky at the point of divorce is extremely unlikely, a complex agreement like a private divorce should be included in the prenuptual agreement.

Following a divorce, each party will have an incentive to reveal the intimate details of your life to others, regardless of your social or economic status. The more status that you have, the more widely disseminated the revelation will be, but even a regular person might reveal all of the gritty details to those in their social circle. The best way to prevent this kind of invasion is to include a non-disclosure agreement as part of the divorce.

CHILDREN

Having children reduces your privacy because you now have other individuals who you are responsible for, and who are not responsible for themselves in many ways.

If you have children, you must teach them privacy principles as well, such as never giving out your home address or phone number. If your children go to public school, it will be impossible to guard this information since it is usually required for registration. Home schooling keeps parents from having to

disclose much of their personal information and is the best option for educating children, but it may also be feasible to find a private school willing to accommodate your privacy wishes.

MAKING PERSONAL PROPERTY VANISH

PRIVATE SAFE

There is a reason why they call it a safe. They could also call it a private. They can be mounted by you or by a professional in a way that prevents theft of the safe itself. You can store anything you want in them and can have any size, like Dick Cheney's man-sized safe, or any number of them in any location you want. There is generally no need to disclose to anyone the contents of your safe or even that you have one.

HIDDEN SAFE

There is even an option of installing your personal safe in a hidden location in your house where it will be less likely to be discovered. This can be placed behind a false wall or in a space under some stairs. Construction skills or a confidential contractor will be needed to install it. When searching for these confidential contractors, make sure that you are hiring a trustworthy company that will take adequate measures to protect your identity on their records.

How To Vanish: High Cost

The tools discussed in this section are not going to be practical for the average person without some significant planning or costs. If you have significant resources, implementing these tools may not require as much planning ahead, but will still be somewhat costly. Many of them, however, will provide you with far more vanishing power than any of the other less intensive measures, and so they are worth considering. In many cases, they are the best thing you can do to vanish completely. If this is your goal, whether it be immediate or for the future, you can smile again, because now you will know just about everything you need in order to do it legally and effectively.

LOCATION

PHYSICAL ADDRESS

You may wish to purchase a used RV with your LLC and park it somewhere. Move to a different location every few months. You will be giving up considerable creature comforts, like space and a cozy bath tub, but your location will be next to impossible to keep track of. The monetary cost of this option is not very high relative to renting or owning property, but the cost in lifestyle change is probably very high.

Another excellent option is to live on a boat. Boat ownership and registration is similar to vehicle registration and can be done in the name of an LLC. Once you own a boat you can rent a space at a marina. Many marinas will allow you to rent a spot for cash as long as the registration of your boat is valid. Most marinas also offer electrical and water service as part of the rental fee, eliminating the need to deal with utility companies. Sewer can either be pumped for a fee or, if you travel the required distance out to sea, you can simply dump it at no charge. I don't know if Shamu would appreciate that, but it is within the law. Move to new marinas, new towns, states, or countries as often as you like. There are no requirements to report domestic boat movement and no speed limit on many bodies of water.

Boat ownership allows you to easily be self reliant and escape the dependency on government services, the biggest obstacle to vanishing. It is relatively simple to convert a boat to use only solar and wind power because they are usually already designed to optimize power usage. Parking a car or an RV in the same spot for a few months is likely to draw the attention of a patrol car or other government authority. Unlike parking an RV or a car, boats can be anchored in a bay or harbor or even off shore for a long time without raising any suspicion by authorities. There are many areas that several boat owners will regularly use to moor their boats. These areas have some distinct qualities that help you vanish. Most boat owners only visit their boat infrequently and so will not easily notice what you, their new neighbor, are doing. If they do visit on a regular basis, or if they also live on their boat, chances are they will be of a similar mind set and enjoy their privacy, and therefore respect your privacy more than most land-lovers. Regular trips to shore can be made for supplies and baseball games. Satellite Internet allows you to communicate no matter where you are, and if you are close enough to shore, wireless Internet

service may be available. You will be limited to coastal regions and waterways, but your ability to move among these areas is very high.

There are several locations that offer a unique opportunity for anonymous camping. Federal lands, BLM land and other places allow you to camp for free if you stay away from the formal campsites, and some places may allow you to stay for an undetermined amount of time. The specific rules and whether it will be closed for some part of the year will depend on which location you select but many will allow you to collect firewood, have a campfire and take water from a nearby stream or lake. You should thoroughly research the area before going there to make sure it is safe, suitable for your needs and to prepare to survive there. There is no registration requirement, no check in, no deposit, and no ID necessary. You will be giving up significant comforts and should do your best to keep the area clean. You may want to move around to different locations within the same or another area to reduce suspicion of rangers and forest fire lookouts. If they notice you they might ask some questions, but they usually will not be able to force you off. If you choose any one or combination of these options, you can set up a ghost address in a nearby town to continue to receive mail at some location.

UTILITIES

There is a growing trend of people going "off the grid." This generally refers to no longer being plugged in to the power grid, but it can mean being completely independent of all utilities including sewer, water, electricity and gas. One common misconception is that you need to move to a remote cabin in the Montana wilderness in order to actually go off the grid. Now, even suburban homes can be completely off the grid. Although there are many reasons to do it, some want to reduce environmental impact, ideological opposition to fossil fuels, or to reduce your cost of living over time, there are significant privacy benefits because you are no longer dependent on utility companies.

I am not going to give an entire how-to on going off the grid, but I will mention the areas that you should consider when going completely off the grid. There will be many variations and possibilities depending on what region you live in. With each case, a combination of low demand appliances and fixtures, changing your lifestyle to reduce your own consumption of the utility, and finding a way to produce everything that you use will depend on both your lifestyle preferences and where you live. Of course you should also consult

your local city ordinances and state regulations to see what is permitted where you intend to live off the grid.

Electricity - In order to get "off the grid" of the power company you need to be able to replace your entire electrical usage with power that you generate. In order to generate your own power, a popular solution is solar power. Installation of an entire solar system, including photo voltaic cells, an inverter, battery storage and/or a standby generator, can be very expensive in the short term, tens of thousands of dollars, but may be able to pay for itself in a few years. Although in some areas you might be able to sell your excess power back to the power company, this does not achieve the complete independence from the utility companies that is the most private.

You might also be able to use, or supplement your solar power with, wind power. If you choose to do this, many of the same system requirements apply to wind power that apply to solar power, but wind is the cleanest source of power developed. Either wind or solar can be easily installed in a remote location or even in residential and suburban areas.

Water - Water can be gathered either through a rainwater collection system or by drilling a well on your property. You may also need storage tanks and other filtration systems or a water ionizer with either rainwater harvesting systems or wells. A wastewater recycling system can be installed to water your yard and for other purposes to reduce the volume of good drinking water needed.

Gas - Propane tanks can be purchased and refilled on a small scale or on a very large scale rather than having a natural gas line to your house. You can also replace all or some of your gas appliances with electric ones so that you do not have to have so many systems, or keep them to spread out the usage. You will have more choice of suppliers, refill times, and who is present to accept and pay for the refill.

Sewer - Instead of a sewer line you can have a septic tank installed. This will allow you to hire a contractor to pump the tank at your convenience rather than being tied to the city's sewer system. You will have freedom and anonymity when you choose to pump your tanks that you cannot have if you depend on the city sewer system.

EXPATRIATE

Because the US legal framework does not permit its citizens to remain private, in fact the law forces many significant disclosures that erode your privacy, you may consider expatriation to a country which does not infringe its citizens' right of privacy. You must first acquire citizenship and a passport from another country.

You can do it the hard way by residing in the country of your choice and abiding by the traditional requirements to become a resident and citizen and acquire a passport. This usually takes a lot of time and may be expensive.

There is another option, you can buy citizenship. Only the Commonwealth of Dominica, St. Kitts & Nevis and Austria offer any kind of program to purchase citizenship. They all have slightly different processes and requirements and have varying costs. There are other travel limitations and considerations which must be weighed before making these an option.

Being a citizen of another nation may, by itself, be sufficient to offer you the desired level of privacy because you can claim the rights of a citizen of the foreign nation. If the foreign nation allows you to claim the right of privacy under more circumstances than may be claimed with US citizenship, you will have increased your privacy.

Remember, unless you fully expatriate you will still be bound by the obligations of both countries of citizenship. This means that Swiss banks might still not accept you as a customer because, your US citizenship subjects banks to disclosure requirements. All US citizens are also taxed on their worldwide income. If you desire not to be burdened by the obligations of a

US citizen, then you need to take the steps to fully expatriate.

Once you have citizenship in another country, you can then take the following steps that are generally required in order to expatriate. You will need to take a voluntary action, like renouncing your citizenship in front of a US consular officer, and have the specific intent to renounce your citizenship by doing so. This can be done by visiting the consular office in any foreign country, not necessarily in the country where you have obtained your new citizenship, and make an appointment with a consular officer to renounce.

After expatriating, you no longer have the right to return to the US. This is a drastic measure that will probably only be worthwhile to a few individuals.

COMMUNICATION

ENCRYPTION

Because strong 256 bit encryption is classified as a munition in the US Code, its commercial distribution in the US is severely limited. Any commercial distribution, even if the actual encryption is provided for free like on Skype, must allow the US government to monitor the traffic. To use 256 bit encryption without revealing the key to the government, you will have to develop your own encryption. This will require the help of programmers, mathematicians and others. The cost to develop will be very high but you will not have to reveal the key to anyone.

ELECTRONIC

PC PRIVACY

If you are concerned about whether the information on your PC is truly private, you can take some very strong measures. Rather than simply reducing your Van Eck emissions, you can take steps to shield them. First of all, do not connect your computer to any wires that are connected to the grid. This means you need to be using your own electricity from a generator or batteries to power your computer. Do not connect it to the Internet or any other networks.

Then, you should construct a space entirely out of solid metal or copper wire mesh like NSA headquarters. Your computer and your power source for

the computer need to be completely enclosed inside the metal structure whenever you need to keep your computer activity private. The effectiveness of this shield will depend on how powerfully you are emitting Van Eck emissions, how thick the metal enclosure is, the thicker the better, and if there are any gaps in your enclosure. In combination with the other recommendations in this book, such as a privacy screen and data encrypted files, this is the most secure you can be while using a PC.

MAKE PERSONAL PROPERTY VANISH

INTERNATIONAL BUSINESS COMPANY/ OFFSHORE LIMITED LIABILITY COMPANY

Your ownership interest in an offshore business entity can keep your involvement from being discovered in the US. You can use that vehicle to set up offshore accounts, trusts, insurance policies and other investment opportunities that are otherwise unavailable to US citizens. Swiss banks, for example, are no longer accepting US clients to open accounts because of the requirements of the USA PATRIOT Act which conflict with their constitutional bank secrecy laws.

There are almost never any requirements for these IBCs to be audited and meetings are not required to be held, like they are for many US entities. Even if meetings are held, they can be held anywhere in the world. In addition, the managers, directors and owners of the entity are usually not disclosed to the public.

Offshore companies that offer ownership to the bearer of shares of the company offer great anonymity because the shares can be transferred privately and there is no record of the owner at all. There are significant tax implications with this kind of ownership so be sure to consult with a professional familiar with these kinds of tax issues when exploring this option. This form of ownership is also highly disfavored by most countries and it can be hard to find a jurisdiction which permits this kind of ownership in a politically stable environment.

OFFSHORE INSURANCE

If you have a significant amount of money to invest, you may want to consider an offshore insurance policy. With large investments, many foreign insurers are willing to customize an insurance policy. The account manager will be able to invest in foreign investments through the policy, rather than in your name. An annuity can also be structured in order to receive disbursements throughout your life. As with other offshore annuities, the payments can be made to you, your spouse or to another designee.

The contract can be written to prevent a transfer of any asset under duress, such as to satisfy a judgment or order of a US court. It can also be structured to make payments in any form you want, either cash, gold, or some other anonymous form.

It is also possible to create an offshore trust or LLC to be the owner of the policy. This has tax benefits as well as providing an extra layer of privacy to the value of your offshore assets. Doing this, however, requires reporting the existence of the trust or offshore business. The privacy that this offers is superb but expensive.

OFFSHORE TRUST

A trust set up in a foreign jurisdiction can have many benefits, one of them being increased privacy over a domestic trust. The trust agreement is entered into overseas and will not be subject to any domestic searches for assets. In addition, usually only the trust name, date of creation and trustee name is recorded. Thus you have similar benefits to domestic trust creation but an added level of privacy because of its distance from your home jurisdiction. These can be very costly to form and maintain and should only be considered if there are significant benefits over other means of protection.

DOMESTIC REAL ESTATE

If you own real property in the US, simply creating an offshore trust to own the property provides little protection from creditors who can see your property and attach it through domestic procedures. One way to avoid this is to use an LLC in combination with the offshore trust. The LLC owns the real estate. The offshore trust owns a very large percentage of the LLC, usually greater than 90%, and you own the remaining portion of the LLC. Thus when there is legal action against the trustor, the beneficiary, the LLC or you, the offshore trust will have the power to liquidate the asset.

How To Vanish: Extreme Cost

Convert all of your assets to gold and silver common coins, live in some remote mountains on a subsistence farm in a 3rd world country. Never speak to anyone again. Only come out at night.

How To Vanish: Bonus Material

Mini Course On Hawala

MODERN HAWALA

That's hawala, not koala. For those unfamiliar with a hawala system, a hawala money transfer is a way to send money via a hawaladar or hawaladars, usually across long distances, at a far lower cost than sending money by wire or bank transfer. Hawala transactions have been used for thousands of years, mostly among African, Asian and Middle Eastern cultures. Although the advent of modern banking has made hawala banking less common than before, the introduction of severe restrictions to banking privacy through legislation and enforcement has made a hawala system a very attractive option again for privately transferring money.

The transfer of money via a hawala banking system is extremely private and is unlikely to be reported or discovered by anyone other than the hawaladar, the transferor and the transferee. In a hawala system, hawaladars are the brokers or facilitators of the transaction. This transactional privacy has made hawala banking an evil villain for enemies of personal privacy and financial privacy. False and exaggerated allegations of money laundering and terrorism funding through hawala money transfers have incorrectly

characterized the hawala network while hawala banking is actually the most efficient and ancient of all money transferring systems.

THE MECHANICS OF HAWALA BANKING SYSTEM WITH HAWALADARS

The most common use for a hawala system is to send money to another person who is at a great distance from you. The money sender contacts a local hawaladar and gives him the money he or she wants to send. The hawladar then contacts another hawaladar in the destination city for the money and arranges to have the hawaladar in the destination city turn over the money to the recipient, minus a small fee. No money actually physically travels the distance at that time but the hawaladars keep a tally of the total owed and then settle the difference at a later date. The exact methods can differ greatly but this is a general overview of how hawala banking works.

BENEFITS OF A HAWALA SYSTEM OR HAWALA NETWORK

The hawala system can exist outside of the traditional legal system because hawaladars generally engage in hawala transactions with other hawaladars based on a long relationship of mutual trust, often built up over generations of hawaladars. Thus with hawala banking there is little need for formal legal protection, which is expensive, and there is a very low risk of default when you transact with such well known individuals.

This hawala system is by far the most private form of transferring money. The entire hawala transaction can occur over a couple of phone calls, emails, text messages, or instant messages. Although the United States requires registration of these kinds of hawala banking services, it is very hard to enforce such a requirement because of the difficulty detecting the hawala transactions. No formal records of the individual hawala transactions are usually kept after the transaction has occurred. All that exists is usually a running tally of what is owed, often encrypted or coded by the hawaladars. This is far different from the extensive disclosures required by banks for a similar transaction.

The hawaladars also have the benefit of being able to settle accounts with something of value other than a currency. These non-cash hawala transactions can be used to avoid currency controls, official exchange rates, import or export duties, or other undesirable tax effects through the hawala system.

These legal, privacy and economic advantages allow the hawaladars to perform the service of a hawala money transfer at a much lower cost than is usually available through bank money transfers.

CRITICISM OF HAWALA BANKING SYSTEM

There are many who strongly criticize the hawala system as dangerous because the transactions are extremely private. The privacy invading aardvarks want to stick their nose in everyone else's business. Although there have been no conclusive findings that hawala transactions have contributed significantly to terrorism or organized crime, some argue that such transactions are likely to do so.

These critics wish to either ban hawala systems (there are strict laws in some states regarding these hawala transactions) or subject the hawala network to rigorous reporting requirements similar to how the banks currently operate. Reporting requirements as they are currently constructed not only offend the notion of justice, but also greatly invade privacy. A search may only occur after a neutral judge finds that there is probable cause and then issues a valid warrant.

Although the banks are subject to invasive reporting requirements, they also require large amounts of capital to operate and thus are not easily overlooked by enforcers of such policies. Hawaladars can easily operate undetected and it is likely that many will do so. Thus the expense of enforcing such regulations could be extremely high. Catching a hawaladar will be as hard as catching a drug smuggler that never smuggles any drugs across the border.

FUTURE OF HAWALA BANKING AND THE HAWALADAR

Because of the dramatic benefits that a hawala system offers it is only a matter of time before it becomes widely used in many more transactions throughout the world. Individuals that act as hawaladars and are well known in their niche or community will grow in influence as they are able to provide hawala banking services at a much lower cost than may be found elsewhere. People who have strong relationships with others in their field of work or in their social life, who have the means to help others with such hawala transactions, will become hawaladars, if just for a family member as a one time

hawala transaction. In addition, the hawala banking services provided by these modern hawaladars will benefit the privacy of individuals.

Hawala Banking And Currency Controls

Hawala banking is a controversial and interesting topic. Although the stereotypical transaction is a remittance of money, there are many other ways to use such as system legally to ones own personal gain in other areas. What are some of those ways?

HAWALA BANKING TRANSACTIONS

There are a few archetypal transactions that most hawala transactions will resemble. The first is the most common; remittances. For example: a person from very poor country X is working in country Y. He sends home $100 USD of purchasing power to his family twice a month. The cost to bank wire this amount is $10 USD or more, a large percentage of his minimal remittance amount. It is difficult to save up and send larger sums on a less frequent basis because banking is unreliable at best in country X and large amounts of cash are not safe to store with his elderly parents, wife and children who are living alone. An exchange through two hawaladars will efficiently facilitate such a transaction on a regular basis at a much lower cost.

The second situation is that of the transactional broker. For example, I

want to buy options on a certain stock but I do not have enough money in my trading account to meet the margin or liquidity requirements. My good friend is planning on purchasing options on the same stock so I give him some money and he buys a few extra options which he will pay me for when I want to cash out. My friend has acted like a hawaladar for the exchange.

A third situation is that of the repatriation or expatriation of wealth. Real estate is a good example because, regardless of legal restrictions, you cannot take real estate away from or add it to a country, with the exception of California which is going to fall into the ocean and Dubai whose palm tree shaped coastline is not a natural phenomenon. If you own real estate in country A but live in country B you cannot simply tuck it into your pocket like a gold coin and repatriate that wealth. You will need to find a buyer of that property to convert the wealth into mobile wealth that can be taken out of country A and brought into country B. Once the wealth is more liquid then it can be transferred to someone acting like a hawaladar for the transaction.

HOW ACCOUNTS ARE SETTLED

The main characteristic of a hawala transaction is that they are informal exchanges made relying on the trust of the parties and generally outside of a structured banking system. In each of these scenarios there must be some settlement made for the transactions. The remitting and receiving hawaladars will maintain a tally of the total amount owed between them and settle their account at a later date. Almost all hawaladars destroy the records of the individual transactions once they are completed. They can then wire the money all at once, or they may simply offset the balance against another account between the two.

What if the debtor on the tally sheet does not have cash to pay the debt? Because this is a private transaction, they may settle the debt using any value they wish. The hawaladars remitting and receiving money might both have sufficient wealth in both countries and will be able to settle their debts with each other through the intra-national exchange of the amount in cash. In addition they might choose not to settle in cash. The hawaladar in poor country X may accept payment in chickens or vampire squids rather than in cash. The friend who bought the option for you might settle what he owes by buying gold for you or a nice steak dinner. The real estate purchaser may not have the cash for the property but gives you his sailboat which is at a slip near your home.

HOW DO I FIND A HAWALADAR?

These situations and a combination of them are representative of most hawala transactions. Now remains the biggest question that I receive about hawala banking: how do I find a hawaladar?

For a person who is not already part of a culture where hawala banking takes place, finding hawala services is not easy but here are a few suggestions.

BECOME A PART OF THE RIGHT COMMUNITY

The main use of hawala is to remit money to the home country of an immigrant worker. Thus you can find where these people are, befriend them and ask to be connected to a hawaladar.

Remember that hawala is a formal name given to an informal system so they might not even know what the word hawala means. Simply look for someone offering the kinds of services you want. Some good communities to look for would be people from Mexico, which receives more money in remittances from the United States than any other country. Middle Eastern countries, East African countries, and South and South Central Asian countries have a long history of hawala practices.

I have had rather good discussions with one person in particular about the cultural barriers to interacting with these kinds of communities. If direct interaction is out of the question, you may need to hire a private courier or messenger to be the intermediary for your search for a hawaladar. My new friend came up with a great idea of hiring a bellhop or a taxi driver because they can move easily in and out of the complex social structures. Another suggestion for those living in a foreign country would be to find a westerner who has a local spouse. The local spouse will likely have more access to these kinds of communities than westerners.

SEARCH ADVERTISEMENTS

Sometimes hawaladars will advertise their services in the local ethnic newspaper. Of course if you do not speak the language of the paper, you may want to hire a translator. A website like Craigslist or other discussion forums might even list some of these kinds of services. It is probably a good idea to

look for the exact services you want rather than the word hawala or hawaladar.

UTILIZE YOUR NETWORK

Ask people you know. Given the financial incentives that may come with the transaction, many people are willing to use their network of friends to engage in these kinds of transactions, especially if it is to help another friend or family member. I have used this method numerous times for all kinds of transactions. A good person to ask might be a friend with a liquid cash position such as a pawn shop owner or a rich uncle.

CONCLUSION

There are significant benefits to hawala banking in many kinds of transactions. Although for many westerners finding hawala services from hawladars on demand may be difficult, the need may become more acute because of the exacerbation of current currency controls and it is likely that these kinds of hawala services will become much more commonplace. In the meantime, it is good to be prepared and have access to those services as soon as possible.

HAWALA BANKING AND CURRENCY CONTROLS PART II

If you are familiar with how hawala banking works then you will probably know that hawala transactions are not inherently wrong and should not arouse any suspicion in the mind of a moral person.

However, there may be formal reporting to government depending on the peculiar nature of some of the assets depending on applicable rules for sale and transfer. In many countries there are legal rules which may impose civil and/or criminal penalties for some kinds of hawala transactions because they are considered money laundering by their governments.

HOW CURRENCY CONTROLS AFFECT HAWALA BANKING

The laws and regulations of various governments regarding financial transactions across the globe cover the entire spectrum from no regulation to very strict regulations. This is not a critique or recommendation based on any particular legal framework but only the fundamental principles surrounding the issue. Therefore, consult a local attorney before engaging in any significant financial transactions.

Currency controls can take many forms. Probably the most common form is the restriction, limitation or prohibition of the sale, purchase or exchange of certain goods or currencies within a country or between countries. Some of these controls include reporting requirements for financial transactions, registration of Money Service Businesses, record keeping requirements when you buy gold or sell silver, and identification requirements for transactors.

The informal nature of traditional hawala banking and the private nature of the transactions allows individuals to avoid interference with their fundamental human rights by currency controls which put a limit on transactions or demand "transparency" requirements. Even so, many nations have made hawala banking subject to these laws, but the laws suffer from these immoral fundamental flaws.

TRANSACTIONAL LIMITATIONS

The limitation, regulation or prohibition of some exchanges makes the goods or currencies like real estate in that they can no longer be freely moved from one country to the next. Things like official foreign currency exchange rates and limits to the amount of cash that can be taken into or out of a country are typical examples.

The solution to this problem, where it is not illegal to do so, is to effect the transaction using one, or a combination, of the examples in Part I. This way the transactional limitations can be lessened or even avoided completely. Nobody likes competition and therefore many vampire squid banks through the governments have made such transactions illegal. Even in the cases shown in Part I, where there is a legitimate reason or purpose behind "avoiding" the transactional limitations, most legal systems which outlaw avoidance would find these methods to be illegal as well.

TRANSPARENCY REQUIREMENTS

Transparency requirements are those laws like the ones found in the ironically named USA PATRIOT Act which require "know your customer" identification requirements, registration with the government to transmit money, record keeping requirements and mandatory Currency Transaction Reports and Suspicious Activity Reports. This framework was suggested by the IMF to governments around the world.

However, these laws are much like the Stamp Act of 1765. In both cases the requirement was unnecessary and used to fund activity which provided no benefit to the people taxed. The Stamp Act was quickly repealed after ardent opposition by the colonists in America. A young John Adams heard James Otis, Jr., a Boston attorney, vehemently speak out about these nefarious Writs of Assistance:

But Otis was a flame of fire! … American Independence was then and there born. The seeds of Patriots and Heroes, to defend the non sine Diis animosus infans;- to defend the vigorous youth were then and there sown. Every man, of an immense crowded audience, appeared to me to go away as I did, ready to take arms against writs of assistance.* Then, and there, was the first scene of the first act of opposition to the arbitrary claims of Great Britain- then and there the child Independence was born. In fifteen years, i.e. in 1776, he grew up to manhood, and declared himself free. [Annals Of The American Revolution Or A Record Of The Causes And Events, page 225]

The fundamental nature of hawala banking, an informal transaction among trusted individuals, makes all of these requirements superfluous and unnecessary for the hawaladars to operate successfully. The history of hawala banking shows that without any of the record keeping and regulation that banks are subject to, hawala banking is far more efficient, less expensive, is not subject to institutional or political risk, has been the source of vital funds for war torn and impoverished nations and is much faster than other systems of exchange. So why force people to use the Pony Express rather than the Internet?

FIGHTING CRIME: Pretending To Be Batman

The competing claims that underlie this clash are between the right to privacy and the protection of innocent people against criminal activity. The argument used to justify the regulation of the informal hawala system is that it is necessary to identify and prevent crime and terrorism. Although it is untrue based on credible and verifiable sources, we will assume it is true that terrorism and organized crime use hawala transactions as a significant source for funding. The question then becomes, how much privacy may be sacrificed to ferret out crime and terrorism?

The Stamp Act opponents relied on the English Constitution for an

argument against the Stamp Act, taxation without representation. The same offenses to liberty and human rights are present with anti-hawala laws but the same constitutional argument is not necessarily applicable here. The stronger one is to look to the US constitution, the Fourth Amendment which states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

It cannot be more clear that in order to protect individuals from crime, before there is a search through private papers, there must be probable cause and a warrant issued to do so.

No transparency requirement as adopted in the USA PATRIOT Act or other financial regulation of hawala banking meets this critical test. Because the transactions are private, there should be probable cause and a proper warrant to search. In addition, the fundamental human right to freedom to contract gives the individuals and the hawaladars the freedom to agree not to maintain records of the individual transaction if they so choose. The same legal argument might not be available in all countries, but the fundamental rights of privacy and freedom of contract are the same for all people.

Thus, just like Batman does not always follow the law to ferret out crime, governments think they can ignore the law and legal principles to fight crime. But unlike Batman, costumed government officials do not actually succeed in reducing crime or terrorism by these means but they do manage to parasitically draw a paycheck from the productive members of society.

CONCLUSION

Hawala banking, where legal, provides opportunities to profit for hawaladars and significant other benefits for the parties to the transactions. Currency controls and other laws passed to regulate hawala banking are not only offensive to fundamental rights of freedom of contract and a right to privacy, but short of complete totalitarian control are impossible to effectively enforce in an informal system such as hawala. The private and informal nature of hawala banking makes detection of hawaladars extremely difficult. And it is the very currency controls that incentivize individuals to use the informal

hawala banking system rather than the formal institutions which are slower, more expensive, less efficient, more intrusive and less secure.

Mini Course On International Issues

THE EXPATRIATE: HOW AMERICANS CAN RENOUNCE CITIZENSHIP

GOING EXPATRIATE

One of the most extreme acts that can be taken by an individual in an attempt to secure more privacy is to renounce their citizenship of the United States and become one of a growing number of expatriates. Although the reasons for expatriation differ, hundreds choose to take this drastic step every year. I will provide you with a brief outline of what the law requires to recognize you as an expatriate. Failure to meet the three part test may mean that you will still be subject to US law as a US citizen, even if you do not intend to be.

US law recognizes the right of any person to relinquish their citizenship.

There is a general principle held almost universally by all nations and that is that "statelessness" is undesirable. Therefore, before you can expatriate, you will need to obtain citizenship of another country. In addition, there are three steps that a person must take in order to renounce US citizenship. A person must 1) take a statutorily enumerated act of expatriation, 2) Do so "voluntarily," and 3) Act with the specific intent of relinquishing their nationality.

ACT OF EXPATRIATION

Some of the acts of expatriation include obtaining naturalization in or taking an oath of allegiance to a foreign state, formally renouncing your citizenship before a diplomatic or consular officer in a foreign state, or fighting in the army of a nation engaged in hostilities against the US.

I hope that I don't have to point out that I do not recommend fighting in the army of a hostile nation. That has the lowest life expectancy of any of the options. Simply obtaining naturalization or taking an oath of allegiance is also a weak option because that in and of itself is done often throughout the world without relinquishing citizenship. There are many who maintain what is commonly known as dual citizenship therefore they are not considered expatriates. The best option is to formally declare that you renounce your citizenship before a diplomatic or consular officer.

VOLUNTARY

Whether you acted voluntarily to renounce your citizenship, or to fight in a hostile army, is presumed. You can of course present evidence that you did not act voluntarily, ie: that you were forced to fight for the Taliban or else be forced to eat nothing but McDonald's for 30 days straight. Since the presumption is in favor of the expatriate, there should be no problem for those wishing to renounce.

SPECIFIC INTENT TO RELINQUISH US NATIONALITY

A formal declaration of renunciation tends to lead to the inference of an intent to relinquish. Therefore the formal declaration kills two birds with one stone. This is not all that is required, however. Other evidence can be used to establish, by inference, that there was no intention to relinquish, even though

an otherwise valid formal declaration was given. Things like returning to the United States soon after your declaration could lead to an inference that you did not have the specific intent to renounce. The person who wishes to expatriate has the burden to prove the act of expatriation and that they had the specific intent to relinquish US nationality.

CONCLUSION

Expatriation is an extreme measure that may not even produce the desired results. You may also still be subject to unwanted tax consequences many years after expatriation. You will also not have the right to enter the US. It may, however, be just what you are looking for.

Fraudulent Identification Documents

FORGED TRAVEL DOCUMENTS

Most people first heard about forged identity documents in high school when some of their friends would try to buy cigarettes or beer while being underage. The black market for forged documents has been around as long as authentic documents.

Forged identity documents have existed since the inception of the insidious practice of impeding the unalienable right to freedom of movement. With powerful personal computers, printing capabilities, etc. the cat and mouse game of document-fraud has escalated tremendously.

A stated goal of the Western Hemisphere Travel Initiative (WHTI) is to decrease the efficacy of forged travel documents. Immigration officials will have to scrutinize a smaller number of travel documents which will be more difficult to alter, counterfeit or obtain through fraud.

There are some physical features such as holograms, ultraviolet patterns, etc. with the more advanced travel documents. But the significant security features in passports and visas come from the linked databases. For a completely counterfeit United States passport the efficacy has been nearly completely eliminated for entrance into the United States although it may still be useful for travel abroad.

Consequently, the ability to Photoshop passports and have them work has been greatly curtailed. Luxury forgers such as intelligence agencies like the Central Intelligence Agency can still accomplish this but obtaining those documents will likely be extremely expensive.

FEDERAL FRAUDULENT FRAUD CASES

To obtain a United States passport a new applicant will generally submit a birth certificate to prove evidence of United States citizenship and a valid drivers license. Relative to a United States passport both of these documents are relatively easy to forge.

For example, luxury alien smugglers with relationships to corrupt officials may charge around $30,000 for a package containing a genuine United States passport, birth certificate, social security card and driver's license or a mere $10,000-15,000 for a genuine United States visa tied to the new database.

The ability to obtain a fraudulent license from a department of motor vehicles (DMV) in a more lenient state presents a significant security hole. Compounding the problem is that an entire illegal industry has arisen to service illegal immigrants in obtaining counterfeit identity documents. Birth certificates can also be illegally obtained fairly easily.

The Diplomatic Security Service (DSS) special agents find a large majority of their fraudulent passport cases involve an application with a fraudulently obtained yet valid driver's license and birth certificate. When these individuals are arrested they often have identification documents for multiple identities from multiple States.

In September 2008 Jose del Castillo, an immigration attorney, who had been indicted on 23 counts of falsely filing immigration forms pled guilty to one count of federal document fraud. He was sentenced to one year in federal prison, fined $15,000 and two years of supervised release.

UNITED STATES VISA WAIVER PROGRAM

Citizens of 35 countries can enter and remain in the United States for up to 90 days without a visa. The countries include European Union member states, Australia, Japan and others. Because these passports are usually easier to either photoshop or obtain a genuine passport from a corrupt government official therefore these passports are at risk of being stolen and carry a premium on the black market.

VALUE OF DOCUMENTS

Many individuals, particularly Americans, are unaware that their passport is worth thousands of dollars on the black market. This can make a group of tourists an especially lucrative target for Third World thieves.

Yet some United States citizens are aware and sell their passports. We do not recommend selling your passport and the reasons should be self evident.

CONCLUSION

Forged identity and travel documents have been around for a long time. While there are increased efforts by governments to increase the security of their borders and travel documents there will always be security holes. The WHTI will assist in closing some of them regarding the use of fraudulent driver's licenses and birth certificates for international travel.

But peddlers of fraudulent documents will evolve their efforts to adapt to WHTI and exploit other weaknesses in the framework. Individuals should be aware of the threat criminals pose to them and their personal privacy. Keep your documents safe, never sell them and be aware of how WHTI affects you.

How WHTI Affects You

FUNDAMENTAL RIGHT TO FREEDOM OF MOVEMENT

The right to travel is a long-standing tradition in Anglo-Saxon law. At Runnymeade on 15 June 1215 King John agreed to the "Articles of the Barons" and a formal document to record the agreement was created by the royal chancery on 15 July: this was the original Magna Carta.

The Magna Carta is the foundation for many modern day constitutions and enumerates many of the protections found therein including the Great Writ of Habeas Corpus. The right to travel was so important it was distinctly set apart in clause 42:

> It shall be lawful to any person, for the future, to go out of our kingdom, and to return, safely and securely, by land or by water, saving his allegiance to us, unless it be in time of war, for some short space, for the common good of the kingdom: excepting prisoners and outlaws, according to the laws of the land, and of the people of the nation at war against us, and Merchants who shall be treated as it is said above.

The United States Supreme Court has long held that freedom of movement within the States is a fundamental right while travel outside the country does not contain the same protections.

WESTERN HEMISPHERE TRAVEL INITIATIVE

The Western Hemisphere Travel Initiative (WHTI) is a particularly annoying program. Remember being able to travel via air into the United States and not need a passport?

In January 2007 the air portion of the initiative went into effect requiring all international travelers to use passports to enter the United States. The land and sea portion went into effect 1 June 2009.

Prior to WHTI American travelers to Mexico, Canada and several Caribbean countries could return to the United States with only a driver's license and birth certificate. The land and sea requirements of WHTI will differ from the air. Valid documents will include passports, United States passport cards, an enhanced driver's license or 'trusted' traveler identification cards such as Sentri or Nexus.

UNITED STATES PASSPORT CARDS

Production of United States passport cards began on 14 July 2008, over 1,000,000 have been issued, applications are usually processed in 4-6 weeks, cost between $20-$45 and the passport cards are valid for 10 years.

If you are a United States citizen with the requisite legal documents then we recommend you apply for and obtain a United States passport card. We also recommend you use this as your primary identity document for activities such as opening a bank account, purchasing prescription drugs when you have a valid prescription, etc.

Merchants sometimes ask for ID when using a credit card although this usually is in breach of the merchant rules with either Visa or Mastercard. Generally, you are not required to provide it and they must still complete the purchase.

A few reasons to use the passport card as your primary identity document is because it (1) does not contain much personal information, (2) does not

contain an address and (3) is quickly and easily recognized.

PASSPORT CARD APPLICATION

The United States Department of State has hired many new examiners because of the flood of passport card applications. These examiners are evaluated based on the amount of applications they process instead of the fraudulent applications they identify. Consequently, examiners issue many genuine passports that probably should not have been issued. It is important to be aware of fraudulent identity documents and how to protect yourself from the criminals that deal in that sphere.

CONCLUSION

The WHTI will impose additional restrictions on the fundamental right to travel and decrease your ability to travel anonymously. The new United States passport card may be more convenient and can help protect your privacy.

Mini Course On Avoiding Surveillance

AVOID VIDEO SURVEILLANCE CAMERAS

Video surveillance cameras are everywhere. What would it be like to be Tom Cruise's character in Minority Report, walking through a public space unable to avoid video surveillance cameras that know who you are? Kinda creepy, huh? This technology is on the verge of widespread implementation around the world. Tommy got an eye transplant in the movie, which solved the problem. Unfortunately, modern facial recognition software relies on several reference points so changing just a few traits, like two baby blues, is usually not enough. I like to have fun. Sometimes that means doing something thrilling like skydiving or bungee jumping, and sometimes that means innocently and harmlessly being a trouble maker. So, in that spirit, lets make some trouble.

Although public video surveillance cameras are found all over the place, especially in large cities and particularly in the UK, they are keeping an eye on

you to make sure you don't do anything you aren't supposed to. Their impact for good is minimal but their potential for misuse is great. What is even more frustrating is the fact that the watchers are trying to keep the watch-ees from watching back. So here are a few of the weaknesses that public video surveillance camera systems currently have.

RED LIGHT AND SPEED ENFORCEMENT VIDEO CAMERAS

Red light cameras and speed enforcement cameras are a big part of the problem. These cash machines are not intended to, and do not increase safety. In many cases they are not properly calibrated or there is a malfunction in the unit capturing innocent people in the cross hairs. In order to avoid being captured improperly, people can first avoid the cameras altogether by knowing what streets and highways to avoid. In the US, photoenforced.com has a great list of these camera systems throughout the country.

If there is a need to frequent these areas, the red light and speed camera systems have difficulty establishing proof of guilt if the drivers face is obscured while near the intersection. Each state and even each judge will have slightly different requirements for conviction, but some simple examples are putting the sun visor down low while in an intersection or wearing a sombrero pulled down low while driving. Some have even driven a car configured for driving in the UK (driver sits where a passenger normally sits in the US) so there will be nobody in the drivers side of the car for the picture. There are some other weaknesses and thoughts at highwayrobbery.net, but be sure to consult an attorney about your unique circumstance before relying on any of them as advice.

VIDEO SURVEILLANCE CAMERAS

There is a really fun feature in NYC called isee which allows individuals to map out the path of least surveillance when walking in NYC. I am surprised that this has not spread more quickly to include more areas. If you can't map out ahead of time to avoid the cameras, a laser pointer aimed directly at the lens of a camera has been shown to obscure the image of many surveillance cameras. This does no damage to the camera. Infra red LED lights can also be used to obscure the image of some video surveillance cameras when aimed at the lens and don't emit any visible light that can be seen by other passersby.

LOW TECH, HIGH EFFECT TO AVOID VIDEO SURVEILLANCE CAMERAS

Like using a low tech hawala system, possibly the most practical and easiest way to avoid being identified on video surveillance cameras is to wear a hooded sweatshirt or coat with your face buried deep inside the hood. Also, most cameras are mounted several feet overhead so looking down helps obscure identity. This is easier done in Minneapolis than in Miami but I'm sure appropriate modifications can be made to blend in with the fashions of warmer climates. Even celebrities use this simple method to do their best to avoid "unwanted" attention.

CONCLUSION

These are just fun observations of the weaknesses of constant public video surveillance. It takes little effort to avoid most video surveillance camera scrutiny. No eyeball transplant necessary.

Transactional Databases

WHAT ARE TRANSACTIONAL DATABASES?

A transactional database is where a database transaction might consist of one or more data-manipulation statements and queries, each reading and/or writing information in the database. These transactional databases can manipulate tremendous amounts of data about our personal lives, habits and transactions.

WHAT IS GATHERED/WHO IS GATHERING?

Most people are aware of the large amounts of consumer and individual information that is being collected by businesses and retailers. Shopper cards, gym memberships, Amazon account activity, credit card purchases, and many other mundane transactions are routinely recorded, indexed and stored in transactional databases.

If you are not paying in cash then the information from the purchase along with your identity is probably being stored on one or more transactional databases somewhere in the cloud. Even if you are paying in cash, if you are using some kind of club card that identifies you as the customer, the information is still being collected. You may not even know that your information is being collected.

BIG DEAL

So what if someone knows what kind of salsa you buy at the grocery store? Who cares if my credit card company keeps track of every expense? I do not do anything remotely scandalous or illegal, so what, me worry?

RISKS FROM TRANSACTIONAL DATABASES

There are several risks to having your activity tracked like this. I will only focus on a narrow area. Many entities are in the business of managing risks. Health insurers take on the risk that their insureds will not get sick, employers take on the risk of the continued performance of their employees. These kinds of entities must trade off the cost of gathering information with the value of the information in assessing the risks associated with the transaction and make the best business decision. Historically, the cost of gathering some information was simply too high to include in the calculation of risk, so these companies chose to transact without the information. They did not have the powerful tools known as transactional databases.

For example, to determine the health of a potential insured, an insurer does not need the private health records of the person. In the past they would have had to follow around the candidate and see what they ate and generally assess their lifestyle. They could then use that information to calculate risk. Because it was too costly to do, they chose not to follow everyone around for a lifestyle audit. They do not have a right to this information, and you do not have to disclose it, but they may choose to gather this information themselves if it is done in public.

MODERN DATA MINING ENVIRONMENT

The cost to investigate and gather information on the risk of a transaction has been reduced dramatically with the maintenance of transactional databases linked to the identity of transacting parties. The lifestyle reflected in your spending habits can tell them all they want to know without hiring an expensive investigator or violating health privacy laws. The cost of your premiums could be significantly increased if it is discovered that you eat cholesterol sticks for dinner with a delicious dessert of artery clog cakes. Insurance premiums might also increase if you enjoy skydiving, para gliding, rock climbing, scuba diving or some of the other activities that make life worth

living.

In both cases the increased information for your counter-party in the negotiation could lead to increased costs for you. These kinds of transactions are a negotiation. The more information that either party can gather then the stronger their position will be. Few transactions are ever done with full information by both parties so there is usually no reason to voluntarily disclose any information to your negotiating counterpart. But transactional databases greatly decreases the costs of storing and retrieving this type of data.

PROTECTION FROM DATA SHARING AND TRANSACTIONAL DATABASES

There are some laws regarding the disclosure of health and other private information. But the legal protection of privacy regarding the disclosure of grocery shopping habits and other things is slim to none in the US. Therefore, you are at the mercy of the self imposed privacy policies of the individual companies you deal with along with your ability to stay out of those transactional databases in the first place.

Given the fact that these privacy policies almost always allow for sharing of information with "affiliates" and, because the standards for becoming an "affiliate" are usually extremely low, there is a serious need to keep the information from being available from "affiliates" themselves. It is theoretically easy for the mega-conglomerate insurance companies to become an "affiliate" of a multi-national, mega insurance company. If you deal with any business like that then your personal data is at risk of being catalogued in transactional databases and sold to the highest bidder.

WHAT YOU CAN DO TO PROTECT YOURSELF FROM TRANSACTIONAL DATABASES

Do not use shopper cards. If you do, use a friend or family member's card. If possible use a pseudonym and ghost address to set up your friend or family member's card. Use cash to pay for items whenever possible and especially when the expense reveals your lifestyle or habits. Think twice before disclosing any information in exchange for goods or services even if it seems harmless because your personal data may end up in some transactional databases.

CONCLUSION

Following these, and other tips discussed on HowToVanish.com will keep you less vulnerable to unwanted disclosures of information that could become, at the very least, an economic annoyance for you. And you never know how long this personal data will be kept in these nebulous transactional databases.

Avoid Private Investigators

How is it that the most nutty character, Dory, in the movie Finding Nemo actually teaches a very valuable principle? Let me assure you, it is not how to speak whale, it is what to do when you realize that you are being followed by a private investigator. There are certain times when it is most likely that you will be the subject of an investigation, ways to recognize that you are being investigated, and ways to "burn" the investigator.

WHEN INVESTIGATION IS LIKELY

Even the Hollywood image of police or private investigators conducting surveillance on a subject make one thing very clear, there must be some reason to investigate the person. The most likely reasons for investigation include when you have filed a claim with your insurance company for personal injuries, if you are involved in litigation, or for divorce or child support/ custody issues. Essentially, there must be an incentive to discover some detail of your private life. Otherwise, hiring an investigator to do surveillance on you is just a very expensive hobby.

The economic resources of the person or entity that might be investigating you is also a clue to how much surveillance is actually being conducted on you.

In a small lawsuit or in an average divorce proceeding, there are probably only a handful of days, 4-5, over the course of several months in which surveillance is actually being conducted and the instruments of surveillance are probably low tech. The higher the value of the case or divorce, the more resources are likely to be allocated to the surveillance, thus more days in the same period of time devoted to it and the more sophisticated the surveillance is likely to be. If there are specific events that are the subject of the underlying dispute, such as visitation days of children when the fitness of the parent is at issue, the likelihood of surveillance on those occasions is much higher. Common sense is a good guide as to when, how and how often a private investigator might be watching you.

HOW TO RECOGNIZE THAT YOU ARE BEING FOLLOWED

Far from the image of two guys parked in front of your house for hours in a sedan, drinking coffee and eating fast food, investigators use much more sophisticated methods to avoid detection because avoiding detection is the name of the game for them. The most obvious signs that you are being investigated are that you see an unfamiliar car in the neighborhood, you notice a car or a person following you, or if you notice a stranger taking pictures or video of you, your property or your neighborhood. Some less obvious signs are that your friends and acquaintances tell you they have received phone calls or visitors asking about you or you get an increased number of wrong numbers or hang-ups. You may also want to check under your car for any tracking devices that might be attached to it. Once you suspect that you are under surveillance, you may then take action to disrupt the surveillance.

HOW TO BURN AN INVESTIGATOR

Many people, upon discovering that they are being watched, immediately engage in evasive action, either overtly or covertly, to lose their investigator. This is especially useful if you think you are being watched but haven't identified the snoop. If the investigator doesn't think they have been discovered, they will simply return another day and probably still get the information they were looking for. If you have identified an individual as a suspected snoop the best way to ruin their case is to confront them about it. This takes some guts, especially if you aren't certain about their activities, but it lets them know that they have been burned. Keep in mind that the investigator will never admit that they are investigating you. Even if you catch

them taking pictures of you they will come up with some lame story about how they grew up in your house and are just reminiscing about old times or something like that. If you are wrong about being followed, you may look weird but there will be no real harm done to the other person.

The key to ending surveillance is to then follow them until they leave. I have no qualms about recommending this because if they can do it to you, you can do it to them. You do not need to hide the fact that you have reversed the roles, it is actually better if they know you are watching them. You may either be up front about suspecting them of following you or pretend that you believe their story and pepper them with questions about the details of what they are doing and why. If their behavior is truly suspicious, you may even be able to notify the police. In either case, the investigation is probably going to end because the investigator has been burned.

CONCLUSION

If you suspect you are being followed, play the game and follow your follower. The best way to do this is to openly confront them about following you, much like Dory confronting Marlin, and then openly follow them until they leave. This will keep your private life a little more private from any investigator that might be interested in you.

VANISHING IN A DIGITAL AGE: LESSONS FROM EVAN RATLIFF

Like many privacy minded individuals, I got a kick out of Wired Magazine editor Evan Ratliff's experiment to Vanish for 30 days. Even though it was a contest and there were many things that he did intentionally to leave some kind of a trail behind, much like what happens to many people who try to vanish, what he did that worked and what he did that didn't work are very illuminating to those who really want to vanish without leaving a trace. Evan was unfortunately caught a few days shy of his 30 day goal. Even more unfortunate is the idea that has perpetuated since the contest, one that many people have mentioned to me since the contest was over, that you simply cannot vanish and maintain a presence on the Internet. This is not entirely true. I have addressed in previous articles almost every tool and technique that would have helped a person avoid the actual mistakes Evan made and which would have kept Evan from being discovered for the entire 30 days or even for 30 years. Here are the things that can be learned from the Vanish contest to make a vanishing act last longer than 30 days.

RESOURCES ALLOCATED TO FINDING YOU

Evan Ratliff publicized his Vanish contest to his readers. Doing this brought lots of attention and got people to allocate their time and talents to the search, a lot of people. The more resources allocated to finding you, the harder

it will be to vanish, but it is still possible (think bin Laden).

Don't make your intention to vanish without a trace known to thousands of people. Ok. It was a contest rather than a true attempt to vanish, so Evan could not have followed this piece of advice, but you can. Being discreet about vanishing keeps resources from being allocated to search for you. If your intention is to vanish because of serious criminal behavior, you will hopefully have a very difficult time vanishing because lots of powerful government and other resources will be deployed in your search. If you are vanishing for honest reasons, the same level of resources will probably not be allocated to locating you and you will find it easier to vanish.

PERSONAL PROFILING OF EVERYDAY HABITS

Using cash instead of credit cards was an excellent method of maintaining his privacy in the short term. Evan allowed others to access his bank account statements, credit card statements, email and other personally revealing information, much like the access a private investigator would have if they were following you. Had he not used cash, his trail would have been completely exposed within hours. His weakness was that Evan has not practiced privacy principles of anonymous transactions his entire life. From his historical spending habits and other readily available personal information, followers were able to compile a profile which helped searchers discover Evan's alias Facebook and Twitter accounts, which kept the trail of his general whereabouts warm, and eventually led them to the gluten free pizza place, Naked Pizza, in New Orleans where he was finally found (his gluten allergy was one of those bits of personal information that was a key piece of evidence to find him).

If you continually practice good privacy habits like anonymous web surfing, using cash in transactions, avoiding consumer databases and others, your personal profile will be very difficult to piece together in any way that might be incriminating. The longer you have been following good privacy principles to partially vanish, the easier it will be for you to completely vanish.

SOCIAL MEDIA MISSTEPS

Evan Ratliff created new social media profiles using some real pictures of himself and used those to leave clues about his whereabouts. Even though his profiles were sometimes "secure", he still added contacts that were people and

groups that were relative strangers to him. Followers of Evan contacted many of those casual acquaintances after suspecting that the profile might have belonged to Evan (the fact that there was such tight security on the accounts actually raised suspicion). They also created their own fake profiles to try and get Evan to connect with them through the social media sites. Those acquaintances, and the fake connections produced information that led to his "capture."

FACEBOOK

As I have mentioned before, social media can be useful if used wisely. Having the desired privacy settings on your account is a good start. The critical part that Evan did not do, in part because he wanted to make the contest fair, was was to screen social media connections, allowing only people that you trust sufficiently with the information that you give them to become part of his network. Only connect with people if you are sure that you know who is behind the profile.

ANONYMOUS WEB SURFING

Evan did, on occasion, use free anonymizing software like Tor, to try and hide his actual physical location. He also used wireless Internet regularly. These were excellent steps which did in fact conceal his location. He did not use it enough. Even though his use of proxy servers did disguise his actual location, he did not always use it while using his fake social media accounts, which some people discovered belonged to him. This allowed his followers to narrow his location to one metropolitan city and eventually to his gluten free meal location.

Tor is an excellent free tool to hide your IP address and was very effective for Evan. Other anonymous web surfing tools can be easier to use and offer more privacy. The more you use these tools, the better you will become at operating anonymously and the more difficult it will be to gather your personal information. Even if there are websites that you would be expected to visit, which a good investigation would be monitoring to see if they can figure out which IP address is yours, anonymous web surfing will probably keep them from discovering that you are even visiting those sites, let alone your actual location.

CONCLUSION

Evan Ratliff's contest was a lot of fun to follow. He did a good job at vanishing for almost 30 days, even with his intentional clues. The conclusion that many people have drawn from the contest, however, is wrong. If you follow good privacy practices discussed on this website, you can vanish in a digital age and still maintain a web presence.

Photo Attributions:

http://www.flickr.com/photos/Tambako the Jaguar
http://www.flickr.com/photos/sleepyneko
http://www.flickr.com/photos/Tom Raftery
http://www.flickr.com/photos/pasukaru76
http://www.flickr.com/photos/davidsonscott15
http://www.flickr.com/photos/pigsonthewinguk
http://www.flickr.com/photos/xploitme
http://www.flickr.com/photos/scragz
http://www.flickr.com/photos/Kivanc Nis
http://www.flickr.com/photos/U-g-g-Boy-(-Photograph-World-Sense-)
http://www.flickr.com/photos/Anonymous Account
http://www.flickr.com/photos/bclinesmith
http://www.flickr.com/photos/The Wandering Angel