HowToVanish.com

BILL ROUNDS, ESQ.
TRACE MAYER, J.D.

PERSONAL PRIVACY

TABLE OF CONTENTS

About The Authors 3
LEGAL DISCLAIMER 4
Introduction To The Importance Of Privacy 5
Is Privacy Dead? 7
Why To Take Control Of Your Privacy Incrementally 9
Remove Personal Information From The Internet 11
Cell Phone Security 14
Address Lookup Versus Your Private Address 19
Avoid Attorney Malpractice, Use Free Encryption Software 21
Should I Pay For Anonymous Web Surfing? 25
Transactional Database And Data Mining 27

About The Authors

Trace Mayer, J.D., author of The Great Credit Contraction holds a degree in Accounting, a law degree from California Western School of Law and studies the Austrian school of economics.

He works as an entrepreneur, investor, journalist and monetary scientist. He is a strong advocate of the freedom of speech, a member of the Society of Professional Journalists and the San Diego County Bar Association. He has appeared on ABC, NBC, BNN, radio shows and presented at many investment conferences throughout the world.

He operates RunToGold.com, HowToVanish.com and CreditContraction.com.

Bill Rounds, Esq., is a California attorney and holds a degree in Accounting from the University of Utah and a law degree from California Western School of Law.

He practices civil litigation, domestic and foreign business entity formation and transactions, criminal defense and privacy law. He is a strong advocate of personal and financial freedom and civil liberties.

He operates HowToVanish.com and BillRoundsJD.com
.

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 To The Importance Of Privacy

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!

Is Privacy Dead?

Some people feel like it is useless to protect privacy. Privacy pessimists already feel the ubiquitous surveillance of almost every action they take. They envision a near future when every thought, word and deed are detected recorded and archived for later reference by anyone who wants to know. The advance of technology makes it seem like privacy is dead.

Privacy Is Dead Because Of Technology?

It is true that technology is advancing to track our every move, often without our knowledge. But technology is also advancing to protect privacy in ways that were not available before. There are already many tools that we can use to protect our private information and most of them are free and easy. Tor, Truecrypt, and GnuPG are three great examples.

Unfortunately, as Julian Assange alluded to following the release of “The Spy Files”, much of the technological effort is aimed at invading privacy. But, if privacy is valuable to people, more and more privacy protecting solutions will become available. If privacy is not valuable, then nobody will read this.

The reality is that privacy protecting technology is usually easier to employ than privacy invading technologies. For example, it is free and only takes a few seconds to encrypt files or emails. To break into those emails, you need a significant amount of technical skill, time and money.

Privacy Is Dead Because Of Social Norms?

Many also look to the changing social norms that seem to punish people who don’t want to participate in social network surveillance. Idiots get paid millions to display their stupidity on TV and on the internet. Governments and advertisers can now track people like the East German Stasi could only dream. But, even Mark Zuckerburg is publicly noting the dangers of social networking. Plus, the Stasi aren’t forcing anyone to use Facebook.

The Law Is Killing Privacy?

The Patriot Act has made constant, warrantless digital searches legal. Telecommunications are controlled by strict regulation, preventing communication without government permission. Your bank accounts are under government surveillance. Death by one thousand cuts of privacy invading regulation is a real problem, but the future is not as bleak as it may appear if we look at the bigger picture.

Americans of Japanese descent have much more privacy now than they did during World War II, even though the law allowing them to be imprisoned based on nothing but their heritage is still valid.
Minorities, while still brutalized by law enforcement, are brutalized much less and enjoy much greater freedom than they did under Jim Crow laws.

Encryption Technology Is A Model For Privacy

The most significant protection from unjust law is the technology that has developed to make the law irrelevant. The history of strong encryption is a good example of this. Strong encryption was developed and used by the US military several years ago. At that time, fearing the power of encryption in the hands of the enemies of the US military, it was illegal to export high level encryption technologies to other countries. It was treated as a munition.

But, other groups outside the US were able to harness the power of mathematics and develop strong encryption on their own. Now, strong encryption is so ubiquitous it is available for free to anyone with access to the internet. The law preventing the export of encryption is as useful as a law preventing people from riding their bike in a swimming pool and was severely relaxed in the US.

Many other technologies are rendering other laws irrelevant.Torrents, Tor, GnuPG and other solutions allow individuals to communicate privately. Financial transactions can take place with Bitcoin across international borders with no limits on value, no declarations, and no ability to restrict a transfer.

Keeping Privacy Alive

As with most things in life, 80% of the benefits of privacy can be attained with 20% of the effort. Focusing on just a few of the most effective privacy tools and techniques will go a long way to protecting a material amount of your personal privacy. Giving up does not do any good.

Conclusion

Privacy is alive. We may not be able to unplug completely from the Matrix, but we can have a material amount of privacy by using a few tools that best fit our situation. All we need is to carve out some areas where we can keep our private files, communicate anonymously and transact anonymously

Other information, like our favorite color and our favorite food can be uploaded to the Matrix without much harm done to ourselves. I have no doubt that in some ways there will be privacy battles that are lost in the future. But at the same time, I have no doubt that many solutions to protecting the most fundamental aspects of human autonomy will be developed. There is no putting the genie back in the bottle for many of the privacy protecting tools that have been, or will be developed. Long live privacy!

Why To Take Control Of Your Privacy Incrementally

I have a good friend who is a former special forces soldier. We sat down to lunch a few days ago and he told me about a lot of the training that they go through. Every special forces soldier gets millions of dollars worth of training making them best trained military soldiers to have ever walked on this planet. He didn't get into anything that he was prohibited from sharing, of course, but I was fascinated by some of the things he shared about surviving capture by an enemy and even torture. There are two fundamental principles that keep soldiers, and anyone else, alive and strong through such an extreme experience: Following the rules and winning small mental victories.

Surviving Capture Rule #1: Follow The Rules

Whether captured by an opposing army, a brutal dictator, a rogue band of narco-terrorists, or some other hostile group, the first rule is to obey your captor. They may or may not care about your survival, but they sure as heck aren't going to keep you alive if you are a nuisance. You are at their mercy and should do everything you can to get on their good side. Complying quickly with their orders is one of the best ways to do this.

They will inevitably have unfair and stupid rules. Violating unfair and stupid rules could lead to severe punishment and maybe even death. The endearing image of Steve McQueen tossing a baseball against the wall in solitary confinement in The Great Escape couldn't be further from the truth. In those kinds of dire circumstances staying alive by following the orders of your captors is the highest priority.

Surviving Capture Rule #2: Win Secret Mini-Battles

Your mental strength is the other essential element to surviving captivity. Surviving physically might be worthless unless you survive mentally as well.

To avoid being broken down mentally you need to find ways to win secret battles against your captors. Although not the best example, one of the POW's imprisoned with John McCain found a way to sew images on the inside of his clothes to win a small victory against his captors. Even in V for Vendetta beat her "captors" and stayed mentally strong by reading the journal hidden in crack of her cell wall. Secretly flipping your captor the bird while their back is turned can be another victory. You did it, they didn't see you do it, you win.

Why Should You Care?

There are very few of us who will be in a position like Elizabeth Smart, Aung San Suu Kyi, John McCain, or hostages of the FARC. It is more likely that we might find ourselves traveling in a dictatorship or even living in a formerly free country that has succumbed to the principles of totalitarianism, where fundamental human rights are not respected by the government.

The world is full of countries that accept torture, order assassination of its citizens that are not even charged with a crime, defend institutionalized sexual assault, and humiliate innocent people by forcing public nudity.

North Koreans, for example, fell captive to their government and need to obey the ridiculous laws as strictly as they can to keep from being imprisoned or publicly executed.

People in these circumstances are captives and need to use the same tactics to survive both mentally and physically. But if they are to survive mentally, they need to find small ways to win little secret victories against their captor.

Obeying Ridiculous Laws

Many laws are ridiculous. If a law violates a fundamental human right, for example, it is ridiculous. It might be better to obey a ridiculous law and suffer a little bit than experience the greater suffering that might come from violating a law. Violating the law gives captors an excuse to do terrible things, often with the support of the public who may be unsympathetic to people who violate the law.

Non-violent civil disobedience is still a common practice and, after exhaustion of all available legal remedies, may be a successful way to combat immoral laws. Be prepared to pay the legal price for engaging in civil disobedience.

You Need Privacy To Win Little Victories

You cannot win little victories like Evey Hammond, or John McCain's cell mate without privacy. The tools and tactics of HowToVanish.com and the book "*How To Vanish"* are essential to helping you maintain privacy in case you might find yourself in one of the unfortunate situations of an oppressed citizen, traveler, or other captive.

If you encrypt a birthday message to your grandma, just so someone else can't read it, you have won a small victory. If you encrypt your grocery list, you have won a small victory. If you shop anonymously with cash and don't use an identifying shopper card to buy your groceries, you have won a small victory. If you watch the latest episode of the Office over an encrypted VPN, you have won a small victory. Burying a gold or silver coin in a place only you know about is a small victory. These small victories will help you survive captivity both physically and mentally.

Conclusion

Stay alive and win small victories. Use the legal tools and techniques from "*How to Vanish*" to do that. If you haven't already gotten your copy of the book "*How To Vanish*", check it out so you have a whole arsenal of ways to win little victories.

Remove Personal Information From The Internet

Tattoo ink and internet ink are very similar. A lot of people are getting tattoos and putting their personal information on the internet. But, both tattoos and information on the internet are regrettably hard to remove. Even good ol' Mark Zuckerberg is finding out the hard way that making some personal information public might be a bad idea.

Whatever the popular trend is, there will always be some people who aren't fond of permanent identifying marks. But what can you do if you have made a few foolish mistakes in the past and you need to remove personal information from the internet? Fortunately, it is a lot less painful to remove some of your personal information from the internet than it is to remove a Mike Tyson Special.

Go To The Source

Removing private info from online profiles is an obvious first step, but there are a lot of websites that share or sell your data without your knowledge. There are ways to clean up a lot of that information too.

There are more websites that will share or sell your private data than anyone would like to count. A lot of the internet is just a big echo chamber. For every website with original content there are tons of other sites copying and repeating what was said before. If you want to take down information, focus on removing it from those sources. This narrows down your action to a few, rather than hundreds, of potential sources.

Intelius and Acxiom are two big data aggregators that are the biggest source for most other websites that share sensitive information on the internet. Removing your information from Intelius or Acxiom will effectively remove it from most other websites too. You may still want to remove personal information from other sites too, just to be on the safe side.

Contact The Sites Directly

Most sites allow you to remove data like address, phone number, and social security number. Every company has a different method and you need to follow their own procedures. They might let you do it online, they might make you do it through the mail. Lots of times they will want you to provide more personal information to prove who you are to remove your information. Here is a list of the main sites where your information might be found with a link to remove your info. You might want to check each one to see how much of your own personal information shows up.

Remove Personal Information From The Internet

Intelius.com

Acxiom.com

USsearch.com

Google.com

Zabasearch.com

Peoplefinder.com

Whitepages.com

Yahoosearch.com

411.com

Whowhere.com

Privateeye.com

Infospace.com

Anywho.com

PublicrecordsNow.com

Addressing The Symptom, Not The Problem

Removing information from any of these sites, even Intelius or Acxiom, is like removing an unwanted tattoo. It is much better to avoid the tattoo in the first place than to try to remove it later. Plus, there are no guarantees that you can even remove it completely. The only way to do that is to know how your information gets in those databases in the first place, and prevent it from ever showing up there.

Where Do These Sites Get All Of This Info

All of these websites collect your information from a lot of places like your online profiles (Facebook, linkedin, match.com, etc.) public records (property ownership records, court proceedings, census data, etc.) job application or resume sites, credit reporting agencies, smartphone apps, entering a sweepstakes to get free stuff, and lots of other sources that they won't even tell you about.

Data is valuable and most organizations that get it, sell it. Selling your information is what made Mark Zuckerberg a billionaire.
Prevent Personal Information From Showing Up On The Internet

There are lots of ways to prevent information from ever showing up in these public sources, and from showing up online.
The best way is to leave personal information blank whenever you are asked to provide it. When you must share information, use a ghost address, pre-paid cell phones, a business entity, and other anonymizing techniques you can find in the book *“How To Vanish*”.

Conclusion

Like tattoo removal, removing personal information from the internet is not perfect. Traces of your personal information online may remain for a very long time. If you already have some unwanted informational tattoos, its not too late. The sooner you get started removing personal information from the internet, the better off you will be.

Cell Phone Security

Cell phones are like drivers licenses. It's really hard to function in the modern world without one, but they reveal a lot of information about you that you might not want to share. Fortunately, most people won't try and verify the weight you put on your drivers license, and there are a lot of great ways to protect confidential information with cell phone security.

Cell Phone Security Is Broad

Unfortunately there are too many service providers, too many types of phones, too many different countries, a lack of fully developed solutions, and not much compatibility across them all to give you one simple solution to your mobile privacy needs. This is an overview of the information that you might want to keep private and a few general ways to do that, mostly for smartphones, but not-so-smart ones can be more secure as well. With this overview, it should be easier to discover and implement your optimum privacy configuration.

Laws are different everywhere. It may be illegal in some places to use some of these cell phone security tools or techniques. Do not use any techniques that will violate the law. That will negatively affect your privacy much more than if you had complied with the law and not used that tool.

Subscriber Information

When you buy a phone, your name is usually attached. You sign a contract or you make payments with a credit card, or do something else that ties all of the activity on that device to you.

Keeping subscription information private prevents corrupt governments from accessing that information with or without warrants, subpoenas or due process to silence dissidents, jail peaceful protesters, and hide abuse. It also prevents hackers and rogue employees from compromising networks and databases to steal the valuable data.

Prepaid Cell Phone – Prepaid cell phones can still be purchased for cash without a contract. Minutes can be reloaded with cash as well. You can use the prepaid cell for all of your communications, or just for the most sensitive communications. After a while, the prepaid phone will probably gather enough data to identify you. Replace your prepaid phone often.

Published Number

Most phone numbers can be found in online directories. Those directories are compiled by the vast amounts of data that thousands of companies gather from their customers. If you give a number to a company, or even give them a call, they probably record that number in their database. Your number then might be shared, sold and copied many times by hackers, corrupt governments, thieves and stalkers.

Your phone number can be a key piece of data to paint a data profile that identifies you and a lot more information about you. Hackers, thieves and overly curious stalkers could easily use your phone number to cause you harm.

Unlist Number – Ask your service provider to unlist your number. Contact the databases that collect this information, like Intelius and Acxiom, and follow their procedures for unlisting your number. Stop giving out your number or give out a fake number to people who don't really need it.

Block Caller ID – Many carriers will allow you to block caller ID so that the people you are calling can't get your phone number. In the US you can block caller ID before an individual call (for a price) using *67.

Call Forwarding – You can sign up for call forwarding that forwards calls from your public number to your private number, keeping your private number confidential. Google Voice is a helpful free call forwarding service.

SpoofCard – With Spoofcard it can appear that you are calling from any number you want, protecting your actual number.

Location

Your general location is constantly triangulated by your service provider's cell towers. Your precise GPS coordinates and the WiFi networks you are close to can be monitored and recorded as well. When you use your device, the location is logged.

Corrupt governments can access this data with or without warrants and thieves can use it to target your house when you are on vacation. The cell phone can also be pinged at any time to determine its location, even if you aren't using it.

Prevent Unwanted Tracking – You can turn your cell phone off to make sure that you aren't connecting to any WiFi, your general location isn't being triangulated, and your GPS coordinates are not being tracked to increase your cell phone security.

Malware can continue to broadcast location information, even when the phone is switched off, although it is not common. To prevent surreptitious tracking, remove the battery.

Data Stored On The Phone

Every phone has lots of information stored on it like contact lists, calendars, text messages, photos, call logs, browsing history and much more. The most basic aspect of cell phone security is securing the device itself.

Corrupt, over-criminalized governments that gain access with unjustified searches could use this information to convict you of ridiculous crimes. Sneaky competitors can get inside information that harms a business if employees and owners don't use good cell phone security. Thieves and snoops could get vital information like bank records, passwords, and many other pieces of information that might be on your device.

Settings – Many phones allow you to adjust settings to store less history on the phone itself. This way your old text messages, call logs and other sensitive items can be less vulnerable.

Password Protect – This isn't just to prevent butt-dialing. This also keeps out the curious. Most thieves, illegal government searches and hackers will easily get around the password protection unless the phone is encrypted.

Delete – Regularly delete unwanted data. Just like a computer, its not really gone until it gets overwritten, but at least novice thieves and the casually curious won't get it.

Don't let your phone out of your sight – All someone needs is a few minutes with your phone to install software or hardware that can overcome almost any cell phone security precautions you have taken. If someone that you don't trust has had access to your phone, you may think twice about trusting it.

Wipe/Remote Wipe – Some phones allow you to completely wipe the phone memory remotely. If your phone is lost or gets stolen, you can make sure that data won't be compromised. Every provider also publishes steps needed to wipe a phone before you dispose of it.

Full Encryption – Full encryption is ideal to make sure that all the data is well protected from all but the most sophisticated attacks. The best encryption is open source, since there will be no entity that could provide a back door. There are few open source options available right now, so using a trusted encryption program is the next best thing.

Partial Encryption – Many smartphone apps allow you to encrypt certain types of data on your phone while the rest of it is not encrypted. It can be tricky to make sure there are no unencrypted copies of the data somewhere else on the phone, but partial encryption can be useful to save certain confidential files. Again, open source is best, but trusted encryption software is also good.

Kryptos (iphone)

CellCrypt Mobile (Blackberry, Nokia)

WhisperSystems (Android)

Protecting Conversations

Usually when you have a confidential call with your business partner, your spouse, your attorney or your doctor, nobody else is invited to the conversation.

Cell phone networks around the world allow governments to secretly listen in on those conversations without a warrant. Rogue employees can listen to those conversations too. There is even a slight chance that malicious software is installed on your phone to capture your voice conversations.

Voice Over IP (VOIP) – Many phones let you use VOIP to communicate over the internet instead of over the network which may be compromised by secret wiretaps. A VOIP app might be available or you can use VOIP through your phone's internet connection. You will still have to trust that the VOIP service is not eavesdropping. Open source VOIP software is best, trusted software is good too. Some common software that is free but not open source is Google and Skype. None of this will stop malicious software on your phone from spying on you.

Antivirus – Although it is still rare, phones can be infected with viruses and malware, just like a computer. But, there is antivirus software for cell phone security, just like for computers. You can use that software to protect yourself from viruses. You can also protect from viruses by not opening suspicious email attachments and not clicking on sketchy links like you would on a computer. You can also make sure to download only trusted apps.

Texting

Text messages are very unsecure. They travel through the network unencrypted, are stored on your device and might be stored for a long time.

Text messages are available to just about anyone who gets any access to your phone like corrupt governments, clever hackers, thieves, and unscrupulous competitors. They get it by accessing the network, accessing your provider's records, accessing your phone, and many other ways.

Secure Text Message App – There are some apps available that encrypt your text messages both in transit and at rest on your device.

Instant Messaging – There are several web based IM programs and IM programs designed for different phones that are encrypted and protect your cell phone security and text communications much better than old fashioned text messaging. Unless the IM software is open source, you still have to trust the source, but it is probably better than trusting a large provider.

Voicemail

Voicemail is stored by your service provider on their server.

Rogue employees, corrupt governments and hackers are the most likely to have unauthorized access to voicemail information.

Encrypted Voicemail – Some VOIP services will also offer encrypted voicemail. You still have to trust the VOIP service, but a small offshore VOIP service is less likely to reveal confidential data than a larger service provider.

Photos

Smartphones not only take photos, but they usually add a lot of hidden data to the picture file, called EXIF data. It can include time, date and GPS coordinates, among other things. Any photo that you email or upload from your phone might have this identifying EXIF information in the file.

Turn GPS Tracking Off – Some phones let you turn off geo tagging in the settings. Turning geo tagging off can prevent the data from ever being added to the picure file.

Wipe sensitive data before uploading or emailing – There are several programs which let you remove the EXIF data from images. That way you can send and share images without sharing the identifying information.

Mobile Apps

Mobile apps let you play cool games and have powerful business tools at your fingertips, but many of them can be mining a lot of data that you wouldn't want to share. Linked-In, for example, stores your username and password in plain text. Since most people use the same username and password in many places, this is very damaging information that is very unprotected. And there are lots more apps that do similar things. Some apps even have malicious code hidden in them.

Use Trusted Apps – Minimize your usage of apps or only use trusted apps to increase your cell phone security. Research what data they access and then use them only if you are willing to share that information and are sure there is no malware in them.

Email

Email is the digital equivalent of a post card. The message passes through the hands of many servers en route to its destination and everyone along the way can read it. At the very least your email provider will have a log of your emails which can be subpoenaed or peeked at by corrupt governments.

Encrypt Email – You may be able to encrypt the emails that you send from your device so that nobody can read them in transit or at rest. If the recipient is also using proper encryption, the message may be protected from end to end.

Web Browsing

Your internet provider can see every website that you visit and they can see every wireless network that your phone connects to. Your browser can see every term you search for.

All of this data is readily available to rogue employees and corrupt governments. In many cases it may be sniffed out by clever hackers and sneaky competitors. Most of this data is also stored right on the phone where anyone that has physical access, even the casually curious, can find it.

Use Anonymous Web Surfing – Some phones let you use VPNs like the Tor network so that your carrier, the web browser, and the websites that you visit can't see where you go on the internet. The VPN records would only be available to corrupt governments if the VPN is in a cooperative jurisdiction.

Conclusion

This is just an outline of what is possible. There is no single cell phone yet available that can accomplish complete cell phone security. You may only be interested in a few features. Figure out what features you want and what is most feasible to protect as much of your confidential communications using your cell phone or smart phone as possible. Check out the book How To Vanish for more tips on protecting your phone communications.

Address Lookup Versus Your Private Address

In one corner we have the vast address lookup databases, pulling in personal information from public records and the entire internet. In the other corner is you, trying to keep your private address from becoming public knowledge. If you are a star on a Hollywood star map, or just an average Joe who wants to separate his private and public life, public records of real estate ownership can make it difficult to protect your private address.

The address lookup sites are usually the heavy favorite, but here are a few tips for the underdog to protect privacy and maintain a private address.

Renting A Private Address

Rent. Renting a house, condo or apartment instead of buying is one of the easiest ways to keep your private information out of public records and out of address lookup sites. Property ownership records are public record, but rental records are not.

Try to rent directly from the owner of the property, rather than a property management company. Property management companies keep records of their units and many of them sell their data, including data of their renters. If you must involve a property management company, smaller ones are less likely to share data.

If you never give out your rental address, use ghost addresses, order utilities and services in another name, among other things, you will remain very private.

LLCs and Corporations To Hold Real Estate

If you own property in the name of an LLC or corporation, the business entity will be listed in the public real estate ownership records. Your name will not appear immediately in those public records. Someone would have to make a separate request to the secretary of state to find out who owns that LLC or corporation. It is not the most solid privacy protection of your private address, but it adds an extra layer of protection.

In many property ownership databases, it is possible to search for ownership records by owner’s name. If you own multiple properties in your own name it will be easy to create an asset profile of you. If you own multiple properties with multiple business entities it will be much harder to create such a profile, especially if each of your business entities exist for the sole purpose of managing one property.

New Mexico is the only state where LLCs are totally anonymous. That means that if you own property with a New Mexico LLC your name can’t be connected with the property in the public ownership records or the business ownership records. Plus, you can own real estate with a New Mexico LLC in just about every state in the US without any special filing or permission.

If you want to be very advanced, your New Mexico LLC can be the only owner of your LLC or corporation formed in another state. That way, when someone queries the ownership of an LLC, all they will get is your New Mexico LLC. It will be a dead end.

Trusts To Hold Real Estate

Another very private way to own property is through a trust. Trusts are commonly used by large developers to stealthily buy up several adjacent parcels of land which they will later develop as one, without tipping off the sellers. They buy each individual parcel with a different trust, established only for the purpose of owning the property and named in a way that doesn't identify the real buyer. Disney used this strategy to purchase the land for Disney World. Imagine the price the last seller on the block could get if they knew who had been buying all of the other houses in the neighborhood.

The most private way to buy real estate using a trust is to transfer the property directly into the trust. This is usually only possible if you pay full value for the property and do not mortgage it. Almost every mortgage company will require you to transfer real estate to your own name first before you transfer it to a trust. This will leave your name in the chain of title forever, so it is not preferable but it may be the best you can do and it is better than nothing.

If You Already Own Real Estate In Your Name

If you like where you currently live and you don't want to move but your real estate is already in your own name, you can still transfer it to a trust, LLC, corporation, or New Mexico LLC at any time. This will leave your name in the chain of title, which is searchable, but at least you won't be the current record owner.

Other Tactics To Prevent Address Lookup

Private ownership and occupancy of real estate is only one part of you game plan to keep your name out of the address lookup databases. You need to round out your skills by mastering other important techniques that you can find in "*How To Vanish"*. Never give out your home address, use ghost addresses, order utilities and services in another name, be careful when you order pizza. The address lookup databases have the advantage of being everywhere, but now you have the advantage of knowing how to beat them.

Avoid Attorney Malpractice, Use Free Encryption Software

Attorneys are supposed to keep their clients secrets in strict confidence. It is probably attorney malpractice to disclose client secrets. And I am not just saying that so you tell me all your juicy gossip. Better privacy helps our legal system work. Free encryption software not only helps attorneys protect client secrets, it may be necessary to avoid attorney malpractice.

Huge Identity Theft Risk

Recently I was scanning information on the latest reported data breaches throughout the US. A data breach is when personal information, like social security numbers, credit card numbers, etc., that could be used for identity theft has been compromised. The Identity Theft Resource Center publishes this figure, along with having a lot of other useful stuff.

The data breaches they report all come from either unsecurely transfering files, accidental compromise, insider theft, theft by subcontractors, or even hackers. And, the report only contains breaches that were reported in the media. As you scan through the document you notice some very disturbing things. First, you see a lot of recognizable names that might have some of your data. AT&T, T-Mobile, Citigroup, Priceline.com, TGI Friday's to name just a few.

The next thing you might notice is that a lot of those recognizable names have had significant breaches where thousands, and sometimes millions, of records have been compromised. Here are just a few of the most notable examples out of 113 pages of breaches so far this year.
Holy data security, Batman!

Company	Number of Records Compromised
Education Credit Management Corp	3,300,000
JP Morgan Chase – Circuit City	2,600,000
AvMed Health Plans	1,200,000
South Shore Hospital (MA)	800,000
Citigroup	600,000
Blue Cross – Anthem – WellPoint	470,000
Affinity Health Plan	407,000
US Army Reservists, Serco, Inc.	207,000
Massachusetts Secretary of State	139,000

Companies You Know And Love Have Had Customer Data Compromised

As you scan the document even more, you will notice that a lot of the reported breaches show a red zero indicating no records were compromised. This is slightly misleading. A red zero means they don't know how many records were compromised. Maybe a big giant red question mark would be more appropriate.

Encryption Protects Data And Offers Better Privacy

There are some other things you might not notice. Hidden away in the data are a few black zeros. These reflect records that were encrypted and so even though there was a breach, the data remained secure. This gives us a hint at just how few companies are actually using encryption effectively.

Free Encryption Software

The low number of companies using encryption software is totally ludicrous. Encryption is incredibly simple to use and there is plenty of free encryption software. TrueCrypt is a free, open source program that provides excellent encryption of data and much better privacy.

If you have never heard of TrueCrypt, any other free encryption software, or encryption at all for that matter, encrypting all of your files will take you a total of about 8 minutes.

How To Use Free Encryption Software For Better Privacy

Go to TrueCrypt.org and download the free encryption software. (1 minute)

Go through the tutorial which will walk you through, step by step, how to encrypt and unencrypt files. Make some dummy document and picture files to practice with. (5 minutes)

Once you are done with the tutorial, encrypt all of your most sensitive files. (2 minutes)

Oh, and here's a tip. Check the total size of the files you want to encrypt and estimate how much more encrypted storage space you will want in the future before you start creating a place to hold your encrypted data. You will need to specify the size of the encrypted file before making it.

Potential Attorney Malpractice For Not Encrypting Data

Now for one of the most disturbing things that I noticed. There are several attorneys and law offices on the list. Holy Attorney Client Privilege, Batman! This can pose some serious problems for attorneys in the near future, if it's not a problem already.

Lawyers have strict rules of ethics that they must follow. Most states prohibit a lawyer from revealing confidential client information. Some states are even more strict than that. Plus, lawyers are supposed to act competently to avoid even the accidental disclosure of confidential information.

Given the ease with which even a computer novice can effectively use encryption, it may become the minimum level of competence that lawyers are expected to use to protect their client's confidential information. Failure to use that minimum level of competence could lead to sanctions for attorney malpractice, malpractice lawsuits, and more. Using free encryption software could help avoid attorney malpractice.

Businesses Owners And Free Encryption Software

Business owners, both large and small, should also take note. There is lots of legislation requiring business owners to protect the data that they collect from customers and clients and to promote better privacy. If it is this easy to use free encryption software to protect the sensitive data that you use and store, it could easily be the reasonable standard of care in a negligence lawsuit. It may even be required by law. Why not spend 8 minutes to potentially avoid millions of dollars in legal fees and damage awards. Even if that is not the standard now, why risk it.

Talk to your attorney and ask them if they use encryption. Talk to the businesses you deal with and ask them if they encrypt customer information. If they don't, email them this article, or just tell them about it. Both you, and they, will be glad you did.

Conclusion

Data breaches happen. They will always happen, even if every one is using encryption. But they will happen much less, and much less data will be at risk if more people use encryption. Judging by the Identity Theft Resource Center statistics, it doesn't look like very many businesses use encryption for better privacy.
If you are a business owner, attorney, or just a concerned client or customer, send this to your attorney, accountant, business partners, and friends. They need to know that data is at risk, they may be held liable for a breach, and prevention will take about 8 minutes of their life.

Should I Pay For Anonymous Web Surfing?

I have already written about proxy servers as a way to protect your privacy while searching the internet. My focus then was on free solutions to anonymous web surfing. Paying for proxy service can also turn your regular web surfing into constant anonymous browsing and there are some distinct differences between using free proxy servers and paying for proxy server access.

Anonymous Browsing and Time

Free proxy servers are constantly going online and coming offline. The availability of any one proxy is sometimes limited to days or even hours. Thus, when you find a proxy to use, the chances are that you will have to find a different one the next time you want to surf the web anonymously. If you are anonymous browsing by proxy every time you use the internet this can become burdensome. Also, many of the free sites whose availability is more reliable, will limit your use to a certain number of searches so you will have to rotate between several proxy sites if you want to search more than their allotted minimum. In addition, the free software that might allow you to surf anonymously can be difficult to understand and use for the average computer user.

Paid proxy servers can reduce your time investment for anonymous browsing to a minimum. The time commitment will be comparable to what you spend on your antivirus software. Most paid proxy services are relatively straight forward to use and will be easy to operate for novice computer users.

Anonymous Web Surfing Benefits: Speed

Most free proxy servers still want to make some kind of profit. One of the ways they do this is by using advertising. The ads can slow or severely restrict your user experience and make using the free sites cumbersome. Another phenomenon, known as the tragedy of the commons, affects this free resource. The idea behind the tragedy of the commons is that when there is a free resource, the public will have a tendency to over-use it. So the free proxy servers are often overloaded with traffic and therefore run slowly, even if there are no ads.

Most of the better paid proxy servers have minimal, if any, advertising and won't noticeably slow down the user experience when using anonymous browsing.

Anonymous Browsing Versatility

Free proxy servers tend to have difficulty displaying some images and many free proxy servers will not give you access to websites which require you to login, such as hotmail, myspace or several other websites. Although there are alternatives which allow you access to most of those sites, many times the free anonymous browsing proxy will only allow access to one of them and you have to change proxies to have access to the others.

Most paid proxies will be able to handle any image and allow you access to any page that requires a login.

Anonymous Web Surfing Security

A computer listed as a free proxy server may itself be a compromised computer. There is even a risk that identity thieves will run a free proxy server and record all of your private data as you enter it. Simply reading up on the server that you intend to use before you use it can help you avoid any problems, but that creates more work for you. I generally do not even use a proxy server unless I a can entrust it with my bank privacy.

A good paid anonymous browsing proxy service will control a network of servers which it routes your traffic through, making your searching more safe. Paid sites will usually be able to run in the background and protect your computer every time you are connected to the internet, making the burden on the user minimal.

Anonymous Browsing and Money

Proxy servers will cost you some money. A normal price will be about $10 US per month. Plus, the service will probably only work on one computer at a time, so if there are several computers in your household, the cost could quickly rise to have all of your computers surfing the web anonymously with a paid proxy server. The potential tax savings from making sure that you are surfing only in tax free states could be tremendous.

Conclusion

Free proxy servers are a great way to do anonymous browsing if you have a little bit of time and technical ability. If you have money, or simply lack the time or ability, a paid proxy server can be a great solution. I have a favorite paid proxy server, but there are many to choose from and a different one might better suit your needs. Creating a complete strategy for how to surf the web anonymously and how proxy servers work can be found in “*How To Vanish*” The Book.

Transactional Database And Data Mining

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 data mine and manipulate tremendous amounts of information 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 data mined 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. Even banking transactions in almost all countries around the world are recorded in special databases, eroding bank privacy.

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 data mining 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 through data mining.

Big Deal About Transactional Databases

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 data mined like this. I will only focus on a narrow area. Many entities are in the business of managing risks. For example, 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. Also, governments may rely on the information in transactional databases to tax you for activities that you engaged in while on vacation outside of the tax free state where you actually live.

For example, to determine the health of a potential insured, an insurer does not need the private health records of the person. They simply 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. 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 With Transactional Databases

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, paragliding, 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 done with full information by both parties and so for much of the information available there is no reason to voluntarily disclose it. 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 for example 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, therefore there is a serious need to keep the information from being available from even “affiliates.” It is theoretically easy for the mega-conglomerate insurance companies to become an “affifliate” 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 in the book ”*How To Vanish*”, the “*Bank Privacy Report*”, and “*Tax Domicile*” 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.