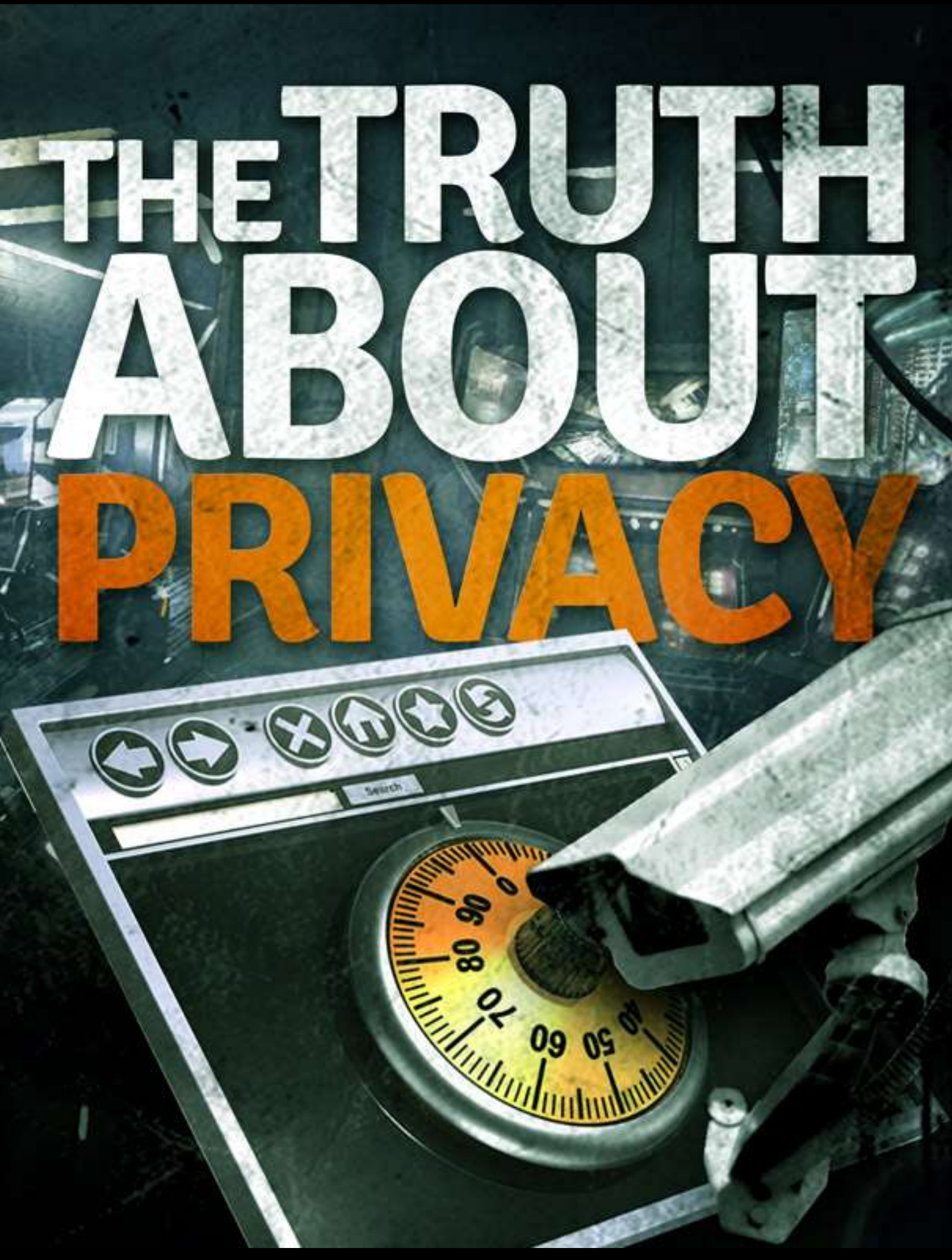

THE TRUTH
ABOUT
PRIVACY
search

DISCLAIMER

The information contained in Patriot Survival Plan, and its several complementary guides, is meant to serve as a comprehensive collection of time-tested and proven strategies that the author of this course has learned over the years, related to survival and preparedness. Summaries, strategies, tips and tricks are only recommendations by the author, and reading this eBook does not guarantee that one's results will exactly mirror our own results. The author of Patriot Survival Plan has made all reasonable efforts to provide current and accurate information for the readers of this course. The author will not be held liable for any unintentional errors or omissions that may be found.

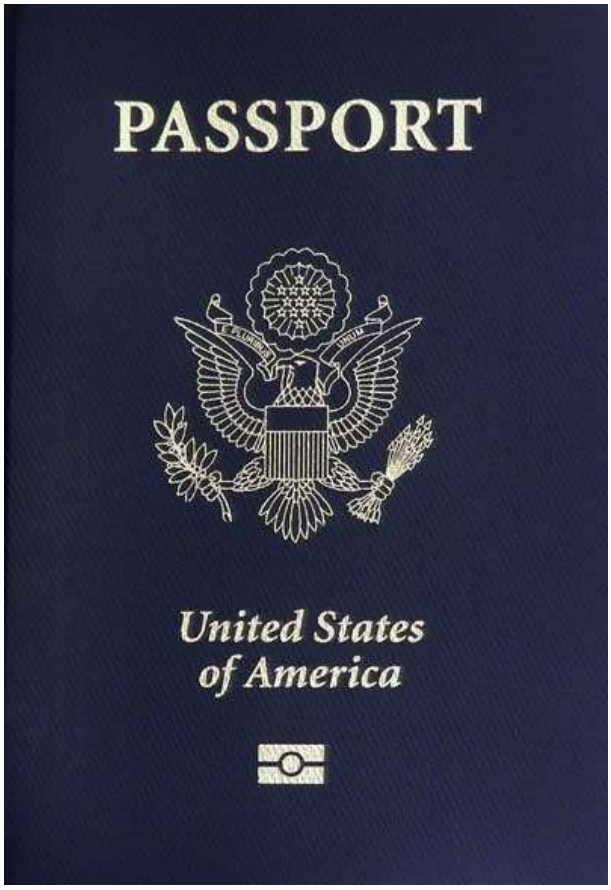
The material in Patriot Survival Plan may include information, products, or services by third parties. Third Party materials comprise of the products and opinions expressed by their owners. As such, the authors of this guide do not assume responsibility or liability for any Third Party Material or opinions.

The publication of such Third Party materials does not constitute the author's guarantee of any information, instruction, opinion, products or service contained within the Third Party Material. Use of recommended Third Party Material does not guarantee that your results, with PatriotSurvivalPlan.com will mirror our own. Publication of such Third Party Material is simply a recommendation and expression of the author's own opinion of that material.

TABLE OF CONTENTS

INTRODUCTION TO THE PRIVACY CRISIS

Everybody wants you. Or rather they want your data, your identity and your credit card and bank information. They want to know what you spend your money on, who you talk to, where you shop, eat, play, work and hang out. They want to know if you like sugar in your coffee, peanuts with your beer and pizza when you watch football.



They want to know more about you than your mother, brother, father, sister or spouse. They want to know what you're going to do before you do it, what you're going to think before you think it and whether you're more likely to commit a crime or be the victim of one. Welcome to the America our forefathers had nightmares about.

Welcome to the exact society our constitution was designed and written to prevent. In other words? Welcome to the privacy crisis. It's not just America. It's every country in the world. As technology and science advances minute-by-minute, so do the assaults, attacks and stealth on your privacy.

Realize that privacy is not just about protecting, shielding or hiding what you do, read, believe or think. Privacy is also about:

Keeping your financial information private and hidden

Keeping your resources (property, money, power, connections etc) private and hidden

Keeping your family safe, protected and shielded from predators, pedophiles, rapists and criminals

Privacy is not about hiding things as much as it is about protecting things. When criminals know your strengths, weaknesses, assets, finances and connections they know how to take, steal, use and undermine your physical, financial and emotional or mental security. You aren't paranoid if you want to be secure. In fact, personal security is such a precious thing that in the United States of America the founding fathers considered it an innate human right. The fourth amendment in the US Bill of rights 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."

The right to be secure. The right to privacy is legally ours, yet our government and other businesses continue to erode the walls of that right. Because most people do not know or understand how to enforce their right to privacy it is slowly being taken away from us.

You can't fly anywhere without being patted, probed and violated by hands, x-rays and procedures. The security measures that were previously limited to airports are now at bus terminals, subway entrances and train stations. If you thought your secrets were safe on your computer, think again.

Give up your passwords or give up your freedom. You my friend belong to the state, to anonymous guardians, bots

and software that tracks everything from your email to your shopping habits. There is no getting past the fact that we have little to no privacy left to us. The only questions left to answer are:

How do we get out of this Orwellian nightmare?

How do we ensure we're not tracked and watched?

How do we get some or all of our rights back?

How do we disappear to avoid being assimilated into the system?

How do we fly under the radar of 24/7 surveillance by an anti-privacy government?

Is it possible to go off the grid entirely?

Is it possible to eliminate, or at least reduce government intrusion into my life?

How much do "they" know and how do I find out if I'm on a death list?

Those are tough questions, but there are answers. It takes work to regain and protect your privacy, but it can be done. It means being dedicated to protecting and defending your rights as well as knowing when to fight and when to walk away and when to simply remain silent.

You can regain an enormous amount of the privacy you've already lost, and you can protect what privacy you currently have, both online (Internet) and off. But you have to educate yourself first. Then you have to set up the systems, controls and behavior that ensure you stay safe.

DIGITAL PRIVACY

Many people who don't have a computer or smartphone believe no one can spy on them or violate their privacy because they're "off the grid" in terms of immediate digital access. But privacy isn't dependent on someone being connected. It's dependent on the people and companies who want to violate your privacy and spy on you.

People, including the government, want to spy on you, keep track of you

and be aware of what you're doing because they own you (the government). They consider you a potential source of income (marketers and businesses), or they want to control you to ensure the people in power remain in power by making sure your politics, beliefs and religious faith don't interfere with their plans for the country.

So, it doesn't matter if you're digitally connected because they most certainly are! They have the software, hardware, resources and knowledge to track you even if you don't own a computer, tablet, iPad, cellphone or digital device. It's harder, but not impossible. Television sets are now made to monitor and report what you watch, when you watch and even your physical reaction to what you see.

NBC news recently reported that Samsung televisions now watch their owners. Their 2012 top-of-the-line plasmas and LED HDTVs offer new features never before available within a television including a built-in, internally wired HD camera, twin microphones, face tracking and speech recognition. On the one hand those features allow you more control over your television, but they also allow hackers or even Samsung to see and hear you and your family, and collect extremely personal data.

Having a web camera and Internet connectivity isn't new, but the total or complete integration with your television is. It's the always connected camera and microphones, combined with the option of third-party apps (not to mention Samsung's own software) that totally blows your privacy away.

Samsung has not released a privacy policy clarifying what data it is collecting and sharing with regard to the new TV sets, so you don't know if your television is on and watching and recording your actions, conversations and activity or not.

And while there is no current evidence of any particular security hole or untoward behavior by Samsung's app partners, Samsung has only stated that it "assumes no responsibility, and shall not be liable" in the event that a product or service is not "appropriate." They also take no responsibility for hackers who are able to access third party apps or your system itself. But would that happen? You bet. It already is.

The privacy violators you need to be aware of aren't always evil criminals or law enforcement types. Would you believe your utility company is spying on you? What about your grocer, the Post Office, your Internet Service Provider (ISP), and even your cell phone company or camera? It's almost impossible in the United States, or most of the world, to have anything remotely resembling the privacy citizens enjoyed post WWI, yes, WWI. By the time WWII rolled around the

Nazis were using IBM computers to keep track of the Jews they arrested. Without IBM, they never could have killed the six million people they annihilated during the war.[7]

If you're online or plugged in to the digital world at all, you have little or no privacy. Maybe your emails, photos and web-surfing history aren't emblazoned on the front page of Google for all the world to see, but the information is there for anyone who wants to go looking, or who becomes curious after reading a Facebook post or hearing a comment you've made.

Don't think it's just the information of private citizens that's out there. Even businesses and corporations can't scrub their information off the Internet or out of government files. That matters because banks, schools, doctors, hospitals, credit card companies and any and all organizations you may do business with, or have done business with, may be published on the Internet.

Read the news. When the IRS recently moved files to new servers and inadvertently published thousands of social security numbers to a public website.

And if the IRS, or even private corporations with all their money, power and connections can't keep things private, what are the odds that private citizens can do much better? The one advantage a private citizen has when it comes to privacy is that they have the power to act quickly and efficiently, to hide, to melt away into the superstructure rather than try to evade, avoid or escape it.

"BUT I HAVE NOTHING TO HIDE..."

It's a hassle to protect your privacy. So why bother protecting it at all if you have "nothing to hide"? Because the greatest threat to your privacy isn't just the government, it's identity thieves, crooks and criminals, pedophiles, rapists and anyone who can turn your lack of privacy into their profit!

Are you a parent? Did you know the GPS and tags on those photos of your children and home you post on Facebook tell pedophiles where your child is—right down to the exact coordinates of their bedroom? Did you know that your child's cellphone can tell pedophiles, or your unhappy ex-spouse, exactly where your child is at all times? Were you aware those strangers or "friends of friends" of people in your social media groups may be pedophiles and criminals posing as friendly people and intent only on gaining access and trust so they can commit their crime of choice?

You say you have nothing to hide, but can you think of a credit card number, bank account, financial information or medical information that wouldn't

hurt you if released online? What about photos your boss, children or spouse might see? Would it affect your job if your co-workers could see how much money you made?

Privacy isn't about hiding something bad. It's about protecting something good. Do you really want people to know how much you make, what you spend it on and how many vacations, trips and purchases you make each year? Do you want your medical records to be open? Do you want your children or family members put in the potential way of gangs, criminals and scammers? No, you don't.

You don't have to see criminals and bad people lurking behind everything online and become a miserable paranoid to protect yourself online and off, but you do need to be aware of the most common ways your privacy is violated and take steps to correct that. Criminals don't like complex, hard to crack, privacy savvy individuals.

They prefer to move on to softer, easier targets. The government rarely pays attention to you or your data unless you enter their radar for some reason. Those two things can ensure you work within the system to remain private and protected. You can go entirely off-grid and disappear, but it takes a lot more work, money and effort. In the meantime, learn to protect your privacy online and off.

OUR PRIVACY RIGHTS ARE LIMITED

In the United States citizens have a legal right to privacy, but those rights are more limited than we might understand. The Fourth Amendment only protects us against searches that violate our *reasonable expectation of privacy*. A reasonable expectation of privacy exists if 1) you actually expect privacy, and 2) your expectation is one that society as a whole would think is legitimate.

Other than that, privacy is a pretty complex concept. Some Supreme Court cases have decided that you have no reasonable expectation of privacy in information you have "knowingly exposed" to a third party — for example, bank records or records of telephone numbers you have dialed — even if you intended for that third party to keep the information secret.

In other words, by engaging in transactions with your bank or communicating phone numbers to your phone company for the purpose of connecting a call, you've "assumed the risk" that they will and may legally share that information with the government. Scary? You bet it is. But there's more.

Every day we "knowingly expose" a lot of information about ourselves, both on and offline, information that we assume is private, but is not. Information collected by third parties— such as your insurance records, credit records, bank records, travel records, library records, phone records and even the records your grocery store keeps when you use your "loyalty" card to get discounts — is information we freely give in order to receive the benefits, discounts or other perks and under current laws, is not for the most part, protected by the Fourth Amendment. The privacy we so adamantly insist is our "right" is practically non-existent, and legally so!

There may be privacy statutes that protect you from some agencies, businesses and medical professionals from sharing information about you — some communications records receive special legal protection, for example — but there is likely no constitutional protection, and it is often very easy for the government to get a hold of these third party records without your ever being notified. If you want your life to remain private, it's up to you to take the steps necessary to ensure that happens.

The Fourth Amendment is a remarkable protector of privacy, but even it won't protect your privacy in certain circumstances:

RESIDENCES.

Everyone has a reasonable expectation of privacy in their home, whether that home is an RV, an apartment, a hotel room or anywhere else they're living— even a tent in a campground or the living compartment of a tractor trailer cab.

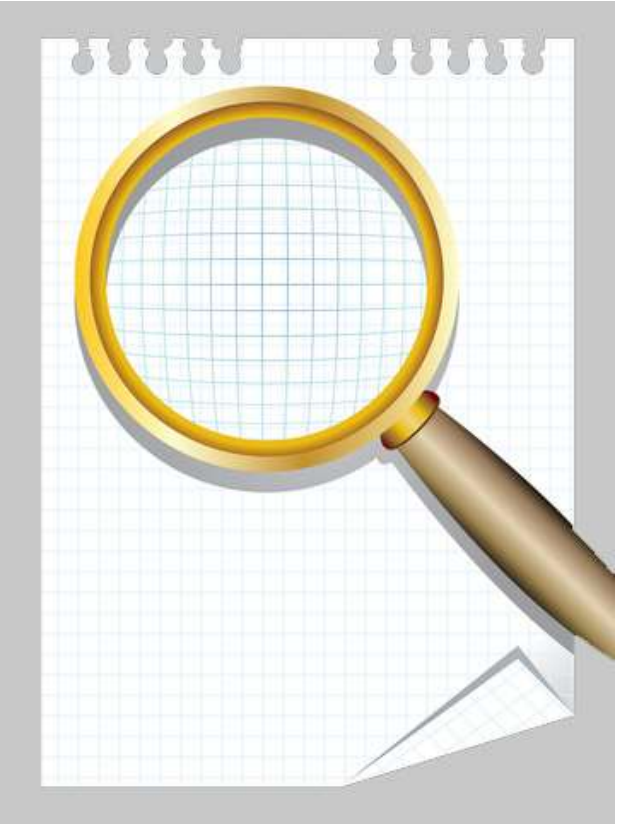
However, even your home loses its Fourth Amendment protection when there are sounds inside your home that a person outside could hear, or odors, like marijuana or drugs that a passerby could smell. If you have an open house, or host a public meeting or event police officers could walk in posing as guests and look at or listen to whatever any of the other guests could, without having to get a warrant.

BUSINESS PREMISES.

If your office is not open to the public you have a reasonable expectation of privacy there. But if the public is allowed into some part of your office, like a reception area in the front, a police officer, reporter or anyone else can enters that part of the office just like any other member of the public is allowed to.

The police can look at objects in plain view or listen to conversations taking place there with no warrant because you've knowingly exposed that part of your office to the public. The police can't go into non-public parts of your

office, like private offices, file cabinets or anywhere not open to the public.



TRASH.

Your trash is public and you have no right to its privacy if you leave it outside your home at the edge of your property. Once you carry your trash out of your house or office and put it on the curb or in the dumpster for collection, you have given up any expectation of privacy around the contents of that trash. Any private eye, detective, cop or government agent can go through your trash without a warrant and use what they find. Criminals can too, although if the information is used in illegal ways you can, if you can prove that, prosecute.

If you're disposing of sensitive documents, magazines, or anything else that you want to keep private consider shredding, destroying or rendering it all unsearchable before setting it out. Or you could wait until the trashman arrives before setting it out. There's no guarantee the trash man isn't a government agent in disguise though, especially if you have a public habit of not setting your trash out like your neighbors do.

PUBLIC PLACES.

You have no expectation of privacy in a public place. When you're out and about, shopping, exercising, driving, working in your yard or anything else you do in public— your actions, movements, and conversations are knowingly exposed to anyone who cares to watch, including the police and the government and any criminal elements around your.

The police and anyone else can follow you around in public and observe your activities, see what you are carrying or to whom you are talking, sit next to you or behind you and listen to your conversations — all without a warrant. Even if you think you are alone, if you're in public your actions are public, so be aware of that. If you want the privacy afforded you by the fourth amendment, you need to find a room, setting or place where you do have an expectation of privacy.

But remember, if people passing by can overhear your conversation, your voice is in a public place and you have no rights to your conversation. So, you may be in a bathroom stall, and have an expectation to privacy, but the conversation you have on your cellphone while in that stall may be overheard by others in the bathroom, making that conversation public. It gets tricky.

INFILTRATORS AND UNDERCOVER AGENTS.

Public meetings, by definition, are not private. If you are part of, or hosting a community or political organization meeting you have no privacy. Even if you're a group of chocolate chip baking senior citizens meeting to discuss parking problems at the nursing home, if the government considers you a potential criminal or terrorist threat, or even if they just have an unfounded suspicion that your organization might be up to something, undercover police or police informants could come to your public meetings and attempt to infiltrate your organization, and they often have.

In spite of laws about recording conversations without other people's consent or knowledge, in a public meeting they may wear hidden microphones and record every word that's said. They can even lie about their identities and never admit that they're cops — even if you confront them and ask them directly if they are.

Police and law enforcement officers or government agents of any organization can infiltrate your organization, identify any of your supporters, learn about your plans and tactics, and even get involved in the politics of the group and influence organizational decisions—all legally.

That's why you may want to save the open-to-the-public meetings your group has for public education and other non-sensitive matters. Limit any sensitive issues in meetings to times when and where you know and trust long-time staff members and others. Meetings don't have to be online affairs. Facebook, Twitter, LinkedIn and other social media sites are often infiltrated by government agents who pose as friends and members in order to access the information on your profile—like your school/university affiliations, former employers, clients and contacts.

We're so trusting we think that our online circle is tight, private and respectful of our privacy, but it's not. The illusion that we're "safe" online is just that—an illusion.

RECORDS ABOUT YOU THAT OTHERS STORE.

You don't really have any privacy when it comes to third party data—the kind Google and other websites collect

from you when you're online. The Supreme Court has stated, "The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."

This means that you will often have no Fourth Amendment protection in the records that others keep about you, because most information that a third party will have about you was either given freely to them by you, thus knowingly exposed, or was collected from other, public sources.

The Supreme Court's ruling means the expectation of privacy on your part, like believing the information you give up to the grocery store, office supply store or even your local gym in confidence, or for a specific purpose, doesn't matter. That's why it's important to pay close attention to the kinds of information about you and your organization's activities that you reveal to third parties.

OPAQUE CONTAINERS AND PACKAGES.

When the Boston Bombers walked through the crowd carrying bombs in their backpacks, they had a reasonable expectation of privacy. Unless police had reasonable cause to believe they were carrying bombs, they had a right to the contents of any opaque (not see-through) clothes or containers. So do you. The police just can't go digging in your pockets or rummaging through your bags for no reason.

Laptops, pagers, cell phones and other electronic devices are also protected by law, even though the government is pushing those boundaries at airports by claiming a right to search electronic devices that hold data. The law has generally treated laptops, cell phones etc. as if they were opaque containers. However, that old "reasonable expectation of privacy" issue comes up here.

Remember that whatever you expose to the public, intentionally or not, isn't protected. So, if you're in a bus terminal, airplane, coffee shop or using your laptop in public and an FBI agent sitting at the next table, or passing by sees what you are writing in an email the Fourth Amendment won't

protect you. The same thing goes to your opening a suitcase, purse, briefcase or bag in public. If someone sees something suspicious, your privacy is out the window.

POSTAL MAIL.

Even though postal clerks have a right to ask you if you're mailing hazardous items, the mail that you send through the U.S. Postal Service is protected by the Fourth Amendment, and in most cases the police have to get a warrant to open it. If you're using the U.S. Postal Service and want to ensure your privacy is protected, send your package using First Class mail or above.

Postal inspectors don't need a search warrant to open discount (media) rate mail because it isn't supposed to be used for personal correspondence. Although the content inside the envelope or package is private, the information on the outside is not.

You don't have any privacy in the "to" and "from" addresses printed on them. That means the police don't need a warrant to ask the post office to report the name and address of every person you send mail to or receive mail from — this is called a "mail cover." Mail covers are a low-tech form of "traffic analysis," or surveillance. You guessed it. Information you put on a postcard, like return and "to" addresses, aren't private either. The government, and anyone who sees the card, can read it.

Can you see now that your life isn't, and has never been, as private as you might have imagined? Privacy is breached every day, whether you are aware of it or not. It's breached, violated and abused both online and offline, so it's important to be aware of how to protect yourself both digitally and physically.

PROTECT YOUR PRIVACY ONLINE

If you truly want to protect your privacy online, then stay off the Internet entirely. If you can't stay off the Internet, stay off of Google. Google is synonymous with Web searching, but it's also synonymous with privacy violation and data tracking. Google keeps track of everything, including your email (which you can't encrypt without using an add-in service like ZipMail for Gmail) Opt out, beg out, get out doesn't matter.

Google relies on your online activity to sell and place its ads, which is how they stay in business. It's not just about the ads. When you search for something on Google, Google sends that search term to the site(s) you click on. They also send that site your computer and browser info. That information in turn identifies you. All that information is compiled into a profile about you. That profile is then sold and can show up in some strange places. For instance, Mac users searching for rooms on Orbitz, are steered towards higher priced rooms.[9]

Makes sense right? Companies assume if you use a pricer computer, live in a higher income zip code, or drive a certain car, you have money to burn. Orbitz, an online travel agency, figured out that Mac users spent an average 30% more a night on hotel rooms than PC users so they started showing Mac users different, and sometimes costly, travel options than they showed Windows visitors. You may also pay more for health, life or other kinds of insurance.[11]

But it's not like Google has a choice. Collecting data is what computers do. They're like our brains, sponges soaking up everything new, only they never forget like we do. Even when you wipe your hard drive and eliminate all the information on your computers, there are dozens, often hundreds of other computers that information passed through on its way to yours that also stored that information. All it takes to retrieve your info is to follow the trail of cookie crumbs. Wherever you go, whatever you do online is monitored, tracked and recorded. Scary isn't it?

Let's say you don't care too much about some anonymous outside agency tracking you. Let's just say you don't want your wife, husband, girlfriend, boyfriend, parents, neighbors and the guy you're selling your used laptop to, to be able to access your browsing history or personal data. It doesn't have to be state secrets, but it may just be personal stuff you don't want the world to see, like banking information, passwords, your Pinterest addiction.

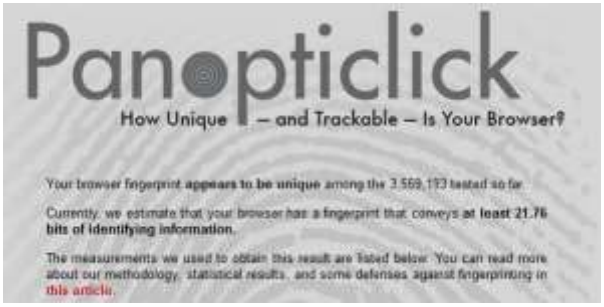
So you wipe your hard drive and throw everything away. You're good, right? No. Not if someone who knows their way around a computer gets their hands on your hard drive. And that means anyone from the fourth grade up these days.

So let's start with privacy 101, Remaining Anonymous Online.

There are a lot of reasons to remain anonymous online. They don't have to be big reasons, or national security threat reasons. You may just not like anyone in your business, or you may want to deter identity thieves and criminals who watch what you do, where you go and then strike when you least expect it, gaining access to your computer, your life, and your identity via the Internet.

How anonymous are you online? Test your browser and see. Go to: https://panopticlick.eff.org/ to find out if your browser configuration is rare or unique. If it is, web sites may be able to track you, *even if you limit or disable cookies*. Panopticlick tests your browser to see how unique it is based on the information it will share with sites it visits. The site gives you a uniqueness score based on your browser, letting you see how easily

identifiable you might be as you surf the web.



Anonymous searches: If you haven't noticed, whenever you search for something, let's say a product or service, ads for that product start to show up wherever you go online. If you haven't noticed that, then go to Google and search on "Penguin Feed" or some off-the-wall product you'd never use.

Then start paying attention to the ads on your Facebook page, or other news and websites you visit. The item you searched on will start turning up in ads. That's because Google sells your searches to third party companies who then target you with ads based on the things you're searching for. They'll also gladly give up a lifetime list of the things you've searched for to any police or law enforcement agency who asks. Another good reason not to let your kids search for bomb making materials, porn or drugs on Google.

An even better reason to be careful about what you search for is related to the profile you develop. If you're searching for information related to mom or dad's kidney problems, diabetes, medication or other health issues, those searches could become part of a profile Google and other sites create about you. Then when you go to buy health insurance or get a job and someone at a health insurance, or other agency checks your online profile, you could be turned down based on your search history without ever knowing why!

Right now the information sold by marketing-database firms is lightly regulated, and no one is really aware of how extensively it's used against or for consumers. Rebecca Kuehn of the Federal Trade Commission's division of privacy and identity protection, says using data in the life-insurance application process would "raise questions" about whether the data would be subject to the federal Fair Credit Reporting Act.

The law's provisions kick in when "adverse action" is taken against a person, such as a decision to deny insurance or increase rates. But you have to be able to show that happened, something that's hard to do unless you have deep pockets and great financial resources.

So if you want your Internet searches to be anonymous, use DuckDuckGo.com, not Google.com, as your search engine. It's too late to do anything about the searches you have made.

You can erase the information on your computer, but the profiles and searches will still exist on hundreds of other servers and machines. But if you do want to sell your computer and ensure information on it doesn't fall into the hands of the buyer or other recipient, you should be aware that simply reinstalling your operating system, or wiping your hard drive isn't enough.

There is software, some of it free, that can find and restore even deleted, trashed or wiped records. Don't worry. It's easy enough to ensure that you do maintain your privacy by erasing your hard drive properly.

ERASING INFORMATION ON YOUR HARD DRIVE

Privacy isn't just about people deliberately wanting to steal your information or records. Sometimes it's about people coming across it when they buy, find or steal a laptop, desktop or other computer. Even though you've deleted or erased your information and files, it's still possible for someone to recover those files with free or low cost software.

Bank records, passwords, social security numbers, your child's school records, your work and personal emails and information—if it crossed your hard drive, chances are it's still there.

If you have a smartphone, you have information on your phone that can also be accessed after you delete it.

If you want to truly erase information you have to do MORE than just drag things to the digital trash and delete them. Even reinstalling your operating system doesn't always work. Why not? When a file is deleted, your operating system removes the link to the file and marks the space free.

Until you overwrite that old information with new information, that file will still exist on your hard drive. Since most hard drives are in the 2 to 8 gigabyte or higher range, it could take months or even years for those files to be overwritten. Your information could remain on the hard drive for years, passing through the hands of numerous hackers. Don't feel bad. Even the FBI and top governmental agencies have had their hard drives released to the public with files still intact. Unless you're a hacker or computer literate and security savvy, chances are very good you didn't know this.

You have to write over the old data so it can't be recovered. To do that:

If you have a PC download the free software program called ERASER, available at: http://eraser.heidi.ie/download.php or buy military and government grade erasing programs like: WipeDrive (http://www.whitecanyon.com/ConsumerWipeDrivePro -

$199 for the professional version and $19.95 for WipeDrive Home version).

CREATE STRONG PASSWORDS

You should have a strong password for every account you have. The temptation to use one password for all your accounts is strong, but don't give in. If a hacker guesses one account it's easier to get into other accounts, but it's still not easy. However, if you use the same password for every account, then you've just handed them your life on a silver platter.

So, create and use strong passwords.

Tips for creating strong passwords:

Use a MINIMUM of eight characters, including symbols, upper and lower case letters, and numbers. Do not use obvious or easy to guess numbers like your license plate, street or work address, phone numbers, birthday or other dates. Do not use nicknames, high school or college names or anything that someone could associate with you if they tried to guess your password or secret questions.

Instead of using a word or name, use the first letter of a phrase or favorite song or quote or bible verse. For instance:

"Happy Birthday to You, Happy Birthday to You," becomes *HB2UHB2U*. That's not quite strong enough, so add a few symbols and make half of the password uppercase and half lowercase, like *#HB2Uhb2u$*

The longer the password the harder it is to guess. If you still need to write it down to remember it, buy a small notebook for just that purpose, and then write it down and keep the book locked in a file drawer, or stored away from your computer. Change your password 3-4 times a year. Good passwords and common sense protection can deter all but the most determined hackers.

Use upper and lower case words, symbols, numbers and random sequences you can easily remember.

LOCK AND CONTROL YOUR COMPUTER

You may not be able to eliminate all the different companies from tracking you online, after all no one owns the web, but Yahoo, Google, Facebook and others control it simply because they're the major players we all have

to go through to do business on the web.

Remember: it pays to be Paranoid. Don't trust any site, no matter how charming, like minded or "professional" it looks. Just because the URL in the address bar begins "https://" and there's a little lock icon in the bottom corner of the browser doesn't mean you can enter your bank-account number, PIN, mother's maiden name, passwords, and the name of your first pet and first car without a worry. Hackers, phishers and criminals can create websites that look safer than the real deal. Unless you know the site, and know it's legit, don't trust it.

Use strong passwords and change them frequently. It's a pain to do, but change them every week, every month or at least every 60 days if you want to stay secure.

If you work for a large corporation the tech guys there can get into any file, email, message or password on your computer. It's what they do and are paid to do. But if you want to keep less savvy, honest or less ethical, nosy or malicious coworkers off your computer when you're away, then learn how to protect it, lock it, clear the history and the cache.

Even when you do everything right, deny permissions and set your security level to high, Google will ignore all that and bypass your opt-out and settings against your will to install tracking cookies on your computer. And they're not the only ones. Microsoft found that Facebook and many other sites are doing the same thing.

So just assume that none of your preferences are going to truly protect you, because they're not. This is happening with cellphones, smartphones, iPads, tablets, lap and desktop computers. NOTHING is sacred or safe unless it's encrypted, and if the stakes are high enough and the government really wants your encrypted files, even those can be cracked.

As the old saying goes, the only safe secret is the one you keep to yourself. Your friends, family, neighbors and co-workers can't keep a secret and neither can your computer or other digital devices, so don't share anything you don't want potentially broadcast or shared with anyone or anything.

Harsh, but true. In the meantime, to reduce the chance your information, files or personal information gets out, take all the precautions you can. You may not eliminate the threat, but you can sure reduce it!

LOCK YOUR COMPUTER WHEN YOU LEAVE IT.

This means lock it when you go to work, to sleep or when you're away from it (work) for any length of time:

TO LOCK YOUR MAC:

Open your Keychain Access utility in the Applications/Utility folder.

Under the View menu, select Show Status in Menu Bar. A black padlock will appear in your taskbar in the upper right-hand corner.

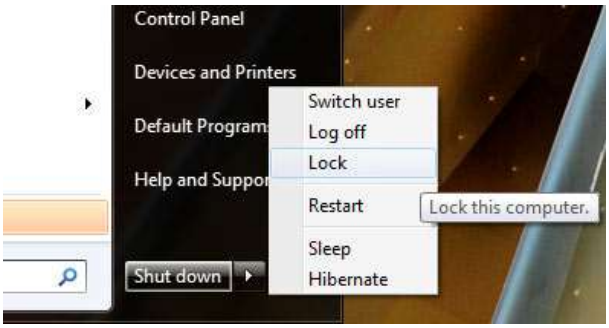
Click on the padlock, you now have a Lock Screen option in the drop-down.

TO LOCK YOUR PC (VISTA OR XP)

Press CTRL + ALT+DEL together.

Windows XP: Select Lock Computer.

Windows Vista: Select Lock this computer.



WHEN YOU LOG OFF OF YOUR COMPUTER. CLEAR YOUR CACHE AND COOKIES:

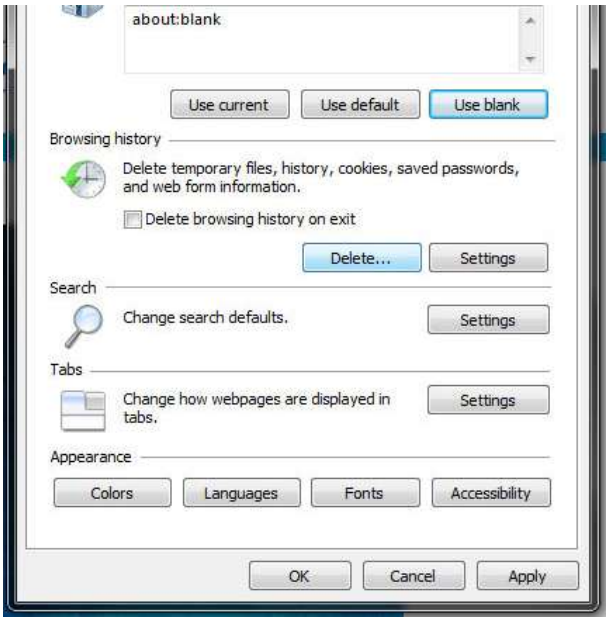
Cookies store personal information. Hackers often use cookies to gain access to your browser and accounts. Set your browser to only allow cookies from your trusted sites, or clear the cookies from your browser when you exit.

INTERNET EXPLORER 8.0+ FOR WINDOWS

Start Internet Explorer, and select the Tools menu (this can be found in the upper right). Then select Delete... in the Browsing history section

Check Temporary Internet files and Cookies

Select Delete.



INTERNET EXPLORER 7.0 FOR WINDOWS

Start Internet Explorer, and select the Tools menu (this can be found in the upper right). Then select Delete Browsing History…

Select Delete files… and select Yes to confirm.

Select Delete cookies… and select Yes to confirm.

INTERNET EXPLORER 6.0+ FOR WINDOWS

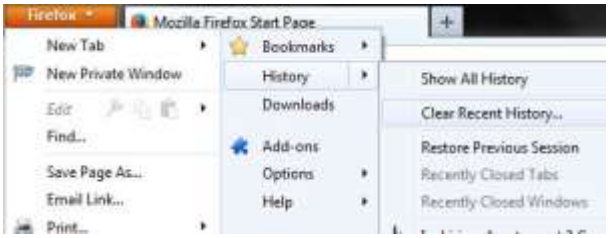
Start Internet Explorer, and select the Tools menu and Internet Options.

Select the General Tab.

In the center of the dialog box under the Temporary Internet Files header, you should see three (3) buttons: Delete Cookies, Delete Files and Settings.

Select Delete Cookies and select OK to confirm.

Select Delete Files, check the box labeled Delete all offline content and click OK to confirm.



FIREFOX 3.0+ FOR WINDOWS AND OS 10.X

Start Firefox, select the Tools menu and Clear Recent History….

Select the desired Time range

Make sure that Cookies and Cache are selected.

Select the Clear Now button.

FIREFOX 2.0 FOR WINDOWS AND OS 10.X

Start Firefox, select the Tools menu and Clear Private Data….

Make sure that Cookies and Cache are selected.

Select the Clear Private Data Now button.

SAFARI 2.0+ FOR OS 10.X

Start Safari, select the Safari menu.

Select Empty Cache.

Click Empty to confirm.

Use an anonymizer. Anonymous proxy servers mask your computer's IP address. It's the IP address most websites want and it's that IP information you don't want them to have. With the right anonymizer you can browse sites without them knowing who you are, or where you are.

It's not a 100% solution, and the pages will take longer to load and you may get annoyed messages that tell you that you can't use the site without permitting the use of cookies, but it's another layer. Some free anonymizing proxy servers are Anonymouse, FilterSneak, SlyUser, Vtunnel, Proxify etc.

If you're going to browse the Internet, don't do it with Internet Explorer.

It's the worst browser for privacy and security, even though it's the most popular browser. Thieves know the average person doesn't know this, so that's where they go. Firefox is the safest browser, but it doesn't mean you'll be 100% safe using it either.

If you're going to buy things online, use a prepaid card you can load with a limited amount of funds, or use PayPal. If you want to go the prepaid card route you can buy them at any Walmart, retail store or pharmacy. Most can be reloaded so you don't lose that $1.57 left on the card because you didn't spend it all. Just add enough money to cover your purchases.

PATRIOTIC GOVERNMENT WORKERS?

Not every law enforcement or government agency is made up of officers and agents hell bent on destroying or violating your privacy. There are millions of brave, courageous and patriotic agents who value privacy, law and order just like you do.

However, there are many who become overzealous in their actions and their interpretation of what their job entails. They, and their supervisors go overboard and get crazy in their pursuit of so-called justice by invading the legal privacy of American citizens.

They violate the Constitution of the United States, or the rights of whatever country they're in, all in the name of "fighting terrorism." The fact is, right or wrong, you're likely to be caught up in their giant web whether you have anything to hide or not.

Understanding how these agencies work, what they were created to do, what tasks and missions they're charged with accomplishing will help you stay off of their radar and avoid any unnecessary encounters with them—encounters that could cost you hundreds of thousands of dollars in legal fees, or even jail time if you can't afford attorneys.

All it takes is for one law enforcement officer or court to deem you a "terrorist" for any reason, or no reason, and you can sit in jail forever without the right to a trial or hearing. Yes, it's that bad. Thank President Barack Obama and Congress for extending the Patriot Act for that.

HOW COMPANIES COLLECT YOUR PRIVATE INFORMATION

You just got home from work, threw dinner in the oven and sat down to your computer to check in on Facebook and see you're your friends have been up to. You "like" a dozen posts or photos, post some comments of your own, and click on half a dozen ads or photos ranging from a product you want to know more about, to watching a movie trailer that looks interesting.

You think it's pretty amazing that the ads and movies popping up on your computer are related to the things you've been thinking about this week. That new car you thought was so cool is now showing up in ads on every website you visit. Those shoes you looked at online last month are there too. Wait a minute. Your boyfriend used your computer last weekend. He said he didn't watch any porn, but why are all these Viagra and condom ads popping up. They never did before.

Welcome to the hidden, secret world of computer technology. You haven't filled out form one, yet someone, somewhere is following and using your personal preferences, interests and conversations to track you and customize their advertising to get you to buy.

Every website you visit, every ad you click, every search you make is recorded. It becomes part of your web history and your personal history.

Google searches on bomb making or explosives or terrorism and you may have a couple of gentlemen in black suits, sunglasses and skinny ties show up at your door with or without a warrant. If you think you can do your searching at the local library, think again. Chances are the librarians will turn you in, or your library card—the one with all the numbers that link you to the books you check out—will alert authorities. It's perfectly legal for libraries to have all that information about bombs, serial killers, pedophiles and murder on file for people to check out and read, but it's also perfectly legal for them to alert authorities when people do check them out.

Companies are collecting your private information. From the RFID chips in your tires that tell sensors where you've been, where you entered a toll road and when, and how fast or slow you drove on it, to what brand of razor you buy and who your favorite blue jean manufacturer is, your life is no longer your own.

Online or off, you have no privacy. Satellites, Google and a variety of cameras, sensors and technology has honed in on every human being in the

world. Your unborn child is in the system before they're in the world—from sonograms to blood type and DNA, we are logged, cataloged and itemized from the moment we become a replicating cell in our mother's womb until we die.

So how you can protect your digital and non-digital privacy? You start by understanding what's out there tracking you and why, by opting out, by saying no, by going off grid, by confusing the system and by either hiding in plain sight, or disappearing from sight. Either way, it's a difficult game to play. But you can do it by learning how to protect yourself and your identity and information both online and offline.

PROTECT YOUR INTERNET PRIVACY

Most of us feel anonymous when we surf the Internet. After all, there's no camera on us and who's going to know who *KentuckyPatriot1954@gmail.com*, or *SilverSister897@yahoo*.com is anyway? We make up names and handles and feel a certain anonymity as we browse the Internet as an alter-ego.

Even with your anonymous name firmly in place, the Internet can collect an extensive personal profile on you within mere seconds of your clicking on a site. Even if you didn't enter your location, specific address, name, email address and phone number it's all available from your Internet Service Provider.

Web 2.0 programming allows site owners to access most of this information through IP addresses. They also use Web browser cookies and tiny image files called Web beacons or Web bugs to determine who you are and what your spending and life habits are.

Not only does your IP information tell marketers who you are, it compares the zip code of your number with the known average income of other people within that same zip code. If you're living in Beverly Hills, Scarsdale, NY or other zip codes with an average income in the millions of dollars, you're going to get different ads and pitches than someone living in rural America where the poverty level is the norm for a given zip code.

In addition to determining your income level website owners can discover your specific shopping habits, what keywords you used to find their site and whether or not you were interested in advertisements on their pages. Newer computers don't rely on where your mouse goes. They have built-in cameras that track your eye movements to see where your gaze lingers longest.

MONITOR YOUR COMPUTER

Your computer is not loyal to you. It doesn't know what information you want protected and what you don't unless you tell it what's private. So, when you click on a website, any website, your "tracking session" begins. From the moment you click on a website until the moment you click away, everything you do on that site is tracked, recorded and noted.

Your IP address, the binary digits assigned to your computer by your Internet Service Provider (ISP), tell the webmaster at the site you just visited what your approximate location, including city, suburb and state is. They even know what kind of computer hardware you're using and what type of operating system you're running. If you don't believe it, ask yourself why sites download Mac compatible or PC compatible software without asking which you prefer? Or if they do ask, whatever system you're running pops up at the top of the list.

Your IP address alone provides a fairly detailed summary of your computer, but they're not the noisiest of the technologies out there.

Cookies: With an innocuous name like "cookies," who pays attention to these real privacy busters? You should. Cookies are small text files that websites leave on your computer. Different sites leave different cookies and there are many names for them, but there are three primary kinds of cookies, session, persistent and third-party ad cookies.

There are three kinds of web browser cookies spring into action when you surf the Internet. If you try to disable them you'll find pages don't work, or your surfing session is delayed or websites crash. That's how they "encourage" you to leave your cookie settings alone so they can track you. The three main cookie types used to track you:

Session Cookies: Session cookies are simple text files that expire once you close the website.

Persistent Cookies: Persistent cookies do just what their name implies. They exists as a text file as well, but they also remain on your hard drive until you delete it, or it expires. These cookies are used when you log in to a site and want to remain logged in for a set amount of time. Sites like Facebook, social media sites, job sites, store or shopping sites like

Amazon.com and so on use persistent or permanent cookies. Their goal is to collect information about you and your Web browsing habits and this is an excellent way to track you. True, they exist for only one domain, but that domain can and may provide your information to third parties who are also interested in you.

Third Party Ad-Serving Cookies: These cookies monitor your Web browsing habits and patterns and then show you advertisements related to your interests.

That's why when your boyfriend or husband browses porn, hunting, car and male themed websites he gets ads related to him; and when women log in the ads they see are related to shopping, food, cooking, fashion and whatever their interests are.

The third-party aspect refers to the fact the website owner places third-party ads on their site, but the actual ad hosting comes from another company. If you have enabled or accepted the third-party cookie (knowingly or not), the company hosting the ad can access your personal information, including your IP address, location, shopping preferences and in some cases your credit card or Paypal information.

You can almost maintain your privacy from these cookies by declining all third-party cookies. The problem is, even though you decline third-party cookies website owners can get around that boundary by using something called "Web bugs." Web bugs are small graphic elements embedded into a webpage. They're used to hide the fact that the page you're on is being monitored in spite of your request it not be. Information collected by Web bugs includes your IP address, what time you viewed the image, and all the information available from other, related or non-related data from other cookies on your computer.

Web bugs can track you as you move from site to site. They not only track you, they create a personal profile of you to feed to their web-techs. If the idea of being spied on by web bugs bothers you, check the pages you visit by going to your browser, selecting "View page source" and seeing if there are images on the page called "clear.gif" or that link to other sites. These are Web bugs. Welcome to big brother.

There are other cookie types as well. For more information on cookies, how they work and what they do, visit the FTC website: http://www.ftc.gov/ftc/cookies.shtm or http://www.whatarecookies.com

CONTROL YOUR PERSONAL INFORMATION ONLINE AND OFFLINE

Companies want to know who you are and how you respond to their

branding. They do this by monitoring your television use, how you use the Internet and how you interact on social media.

They collect data on everything you do. It's how they decide how best o market and sell their products to you. They use the data to determine what products to create, what products to toss and what products to push, all based on consumer behavior. That doesn't sound so bad really, or does it?

Without this information, companies can't make the products or tailor their services to meet your needs. So that's a good thing. It benefits us by helping reduce costs and provide better products. On the other hand, having your every action online monitored, recorded and tracked and then stored in a database for eternity can make you feel fairly vulnerable, especially when you realize that any government agency only has to request the information these companies have on you to see what you're doing.

They don't even have to tell you they're looking at your browsing history. So what, you say. "I'm not doing anything wrong, why should I care?" Well, if you or your son or daughter does a school report on terrorism and accesses several terrorist sites; or you son wants to show his ROTC class how IEDs are made, that kind of browsing history could be construed as being terroristic.

After all, Jared Marcum, a 14-year old West Virginia teenager with no history of any kind of issues or problems in school was recently arrested and deemed a terrorist by local police for wearing, and refusing to remove a t-shirt that said "NRA—Protect Your Right" and had an illustration of a gun on it.

School policy did not forbid wearing such a shirt, but a teacher was offended when Marcum refused to take the shirt off. The teen is now facing a year in jail and fines.[1] The point is, it's not what YOU think is threatening, but what the government, or teachers, or the police, or even your power company thinks is a threat.

However you feel or whatever you think about the sites you visit, there are distinct ways companies collect your private information when you browse online, and specific ways they use that information. It is important to know exactly how that process works.

PRIVACY HERO TO PRIVACY WHORES

Until recently information technology wasn't a very regulated industry. That changed, somewhere around the time when Google and other major Internet companies like Yahoo, Microsoft and Facebook and Apple crossed over to the dark side and began collaborating with the government rather than resisting them. The very companies,

individuals and organizations we thought were on our side, switched teams.

A VERY BRIEF HISTORY

In 2012 Congress was poised to pass laws intended to protect intellectual property and prevent online piracy. Major and minor tech companies, led by Google, struck back with one of the most effective lobbying tactics ever used: they shut down for a day. The tactic worked and the bill was defeated. But the push by the government wasn't over. They backed off and changed tactics, recognizing you get more of what you want with honey and incentives than fear and threats.

Government lobbyists, insiders and regulators used a different kind of leverage with the tech companies—they pushed the positive, or upsides of working with the National Security Agency, the CIA and with Washington.

After all, aren't hackers only doing the same slimy things the CIA is doing, like hacking into places they're not welcome or allowed, violating privacy and stealing people's information? Money talks and even in Silicon Valley where money flows freely among tech companies, Washington got the attention of companies like Google, Microsoft, Yahoo, Facebook and Apple.

Once companies realized the potential influence of tech money on society, they started freely giving vast amounts of user data to the government's chief surveillance agency. After all, if you can bring down a conservative politician or constituency by handing over some data, why not? It's not so much that these companies are collecting the data, it's that they're sharing it and we don't know why, or with whom, or for what ends.

DRONES

Government agencies have always had the latest and greatest technologies, thanks mostly to advances in military warfare. So it's not surprising that the most popular and powerful technology to come out of the latest war to be used the privacy battles is the drone.

WHAT IS A DRONE?

Drones are an unmanned aerial vehicle or UAV. On a more well known level, they are simply remote controlled aircraft, or RCA's. RCAs have been around for decades and have been a wildly popular hobby for millions of Americans who dream of flying.

RCAs consist of a model airplane, helicopter, UFO looking object or anything that can fly with the help of a small working engine. They range in size from jumbo jet to bumblebee. Indeed, some drones are actually built and look like actual birds and even fly in flocks with real birds.

So, whether you call them UAV's (military term) or RCAs (hobbyist term), a drone is an unmanned aircraft controlled by a computer or by human being on the ground using wireless technology to send radio signals to the aircraft. Although there have been models and working craft since WWII, it wasn't until October of 2001 with the introduction of drones into Afghanistan that the military began to realize their potential.

Drones are launched, deployed or used primarily for military applications, but Realtors and engineers and other businesses use them as well for taking photos, surveilling land or getting visual access to areas that are difficult or impossible to access by land.

Some radio and television stations are using drones for traffic reporting and news gathering, although that's somewhat rare. As cost and familiarity with drones increases the use of the craft for a variety of legitimate, non-invasive uses will probably increase. The only thing is, you won't know if a craft is private, business or law

enforcement. It will be difficult to tell which ones have cameras and which ones have cameras and guns.

Drones used in military operations are famous for the ease in which they can sneak up on, and fire on people on the ground. They are killing machines and that's what most people fear most—that drones will be used by police to kill, fire on, or hurt citizens.

They fear that because in recent years police departments, Homeland Security and various government agencies have also started using drones to watch US citizens. Having an extra and armed "eye in the sky," will "make the population safer," is what law enforcement claims.

The problem with using drones in a war or in peacetime, especially a drone that's armed, is that the operator cannot tell if a person is a "friendly," an innocent by-stander, a criminal, a suspect, or a person of interest.

There have been deaths of American soldiers in war zones by their own drones—casualties called "Friendly fire." The same scenarios will happen in America with the death or harm of American citizens. Even police officers on the scene of a crime often shoot innocent bystanders because they don't know who they're shooting. Putting a gun in an aircraft 20 to 100 feet in the air won't make the decision to shoot any easier.

WHO MAKES THEM?

Lockheed Martin, famous in conspiracy circles for their billion dollar contracts with the US government, makes many of the drones used by the US Military. Lockheed Martin received $36 billion in government contracts in 2008 alone, more than any company in history.

It now does work for more than two dozen government agencies from the Department of Defense and the Department of Energy to the Department of Agriculture and the Environmental Protection Agency. It's involved in surveillance and information processing for the CIA, the FBI, the Internal Revenue Service (IRS), the National Security Agency (NSA), the Pentagon, the Census Bureau, and the Postal Service. According to some, Lockheed Martin is involved in almost every transaction Americans have on a daily basis, from monitoring your mail, your fingerprints, your purchases and of course your Internet use.

WHAT DO THEY CARRY?

Drones can and do carry anything from weapons, to cameras, navigation equipment, night vision cameras, video and still photography cameras, bombs, lasers and missiles. They're very versatile.

HOW MANY ARE THERE?

According to NOVA, who recently produced an extensive and detailed documentary on drones, the USA has more than 10,000 drones in use for military purposes, mostly for spying, but also for killing. One of the most popular drones for military use is a small plane called "The Raven." With a 3-foot wingspan it's both easy to deploy, to transport and to maneuver from the ground.

The most used drone is an MQ1, called "The Predator," and for good reason. Another popular drone is the MQ9, called "The Reaper," and responsible for the deaths of thousands of people in various war zones.

WHO USES DRONES?

The CIA, the US Military, Homeland Security, law enforcement, Realtors, photographers, film makers, hobbyists and engineers among others. The US Border patrol uses drones to look for illegal aliens, but also to search for lost hikers. There are some agencies who are exploring the use of drones to drop food, water and medical supplies to villiages in third world countries and to illegal aliens trying to cross American borders. There are many positive, humanitarian uses for drones, but just as many uses for spying and hurting citizens around the world.

The Coast Guard can search larger areas and longer ranges for lost boaters, or drug smugglers with drones. Search and Rescue crews can also search for victims four times longer, with less risk, less fuel cost and better visual abilities (filming their search).

There are hundreds of excellent ways and reasons to use drones domestically. With the cost of basic remote control or hobbyist unmanned aircraft starting at $500 (or less), it doesn't take much to become a drone pilot. Unfortunately, as with every technology invented, someone will find ways to use it for evil as well.

Pedophiles can use drones to watch children on a playground, or to follow them home without being seen. Criminals can use drones to "case" a location for cameras, security and watch dogs. Peeping Toms can now spy on people in high rise buildings. Rapists, muggers or criminals can work in teams to spot and alert each other to potential victims.

Hijackers or Interstate criminals can target tractor trailer trucks and transportation routes. Terrorists can send drones into the air and interfere with, or shoot down planes. The potential for abuse of drones is endless. And because there are no regulations for many scenarios, it's almost impossible to tell if an RC or UAV is from a law enforcement or

government agency, or a hobbyist or a criminal with illegal intentions.

While the technology has made great strides, the law has not. In 1946 the Supreme Court ruled that the air above the minimum safe altitude of flight "is a public highway" and not subject to trespassing laws. That ruling applied to manned aircraft and meant 500 to 1,000 feet depending on congestion and other factors. Smaller craft, like powered parachutes, hot air balloons etc. may fly even lower.

This means if your neighbor wants to fly his remote controlled plane over your backyard and watch you skinny dipping or sunbathing, he's well within his rights to do so.

FIREPOWER

Cops and law enforcement officers carry 9mm, .45 caliber handguns, shotguns and other weapons capable of wounding or killing a human being. Drones typically carry firepower capable of destroying tanks, car engines or blasting through 4-to-6-feet of concrete. They also carry bombs, lasers and automatic weapons that fire bullets the size of your hand. They are actually more accurate bombers without a human being in the aircraft.

HOW EFFECTIVE ARE THEY?

The Air Force says drones are so effective that they predict up to one-third of their planes will one day be drones.

Effectiveness is in the eye of the beholder. Critics of the drones say that up to 30% of those killed by drones in border wars in Iraq, Pakistan, Yemen and Somalia were innocent civilians. So can they kill? Definitely. Are they capable of distinguishing between who they're killing? No. Not so much. The visual sensors are limited and the military admits that the person flying the drone remotely is not able to see the big picture, only their target. Imagine being in battle and only being able to look through a giant straw instead of having a wide-range of vision.

You can certainly hit the target, but you don't have the advantage of seeing what is happening around that target. For instance, you could shoot a criminal because you weren't able to see police on the ground surrounding him and back off.

Operators can't really tell the difference between a stick, an umbrella and a rifle either. In Afghanistan operators killed 23 women and children because the operator couldn't tell if one woman was holding a stick or a rifle. Yet, the drones have very high resolution optics and can spot something as small as six inches on the ground. They can see people walking, crossing a street, waving their arms or sitting down.

CAPABILITIES

The Predator Drone can spot people on the ground from 5-to-6 miles away, long before the person can hear or see the drone. It can fire on people from the same distance. Accuracy is within 9 feet of the target at that distance.

WHY USE DRONES?

Drones are more accurate, more cost efficient, protect personnel and pilots more effectively and are cheaper to make, fly, use and transport. They can stay in the air longer (up to 24 hours or longer compared to the average 2-to-4 hour flight time for a manned aircraft). They are cheaper to replace if shot down. They are silent.

Most people never know the drone is in the area until the drone fires on them. Civilian users like drones for the same reason the military and law enforcement does—cost. Cost of fuel, cost of the aircraft, cost of personnel, cost of transportation and so on.

Another advantage to using drones is the agency who deployed it can stay around to watch what happens after their strike. If you drop an incendiary device on a marijuana field, you can watch it burn, or watch to see who comes out of the field after. If you are dropping or spraying chemicals on a crowd or riot you can see where agitators run after they're hit. In other words, you don't just drop your load (bomb, bullets or bio agents) and leave.

It's not just the United States that is using drones. More than 55 other countries are looking at ways to introduce drones into their systems as well. According to a CCTV user group and various British media reports, has an estimated 1.5 billion CCTV cameras are in use throughout the United Kingdom. That's one camera per every 32 citizens.

WHAT'S NEXT?

Drones now rely on things like satellite links and radio waves. They can be hacked, and indeed several groups have claimed they were able to jam signals, or hack into the drone's computers to crash or capture the drone.

In Pennsylvania researchers are currently working drones that are self-sufficient. Their controls are self contained and they don't need to rely on satellite links to get their flying instructions. Gyroscopes act as sensors to tell the plane to right itself, slow down, speed up or take other actions—just as a human's innate sensory abilities would do. If a person riding a bike feels a loss of balance their brain alerts them to move in ways to restore that balance. Now drones are being developed that do the same thing.

When the robots systems in the drones are in place, the drones will have a

definite advantage. As incredible as the human neuromuscular system is, there may be delays of the order of 80 milliseconds or 200 milliseconds before a person can act on what they're seeing. Robots in the drone can do the same calculation or computations hundreds of times a second every time. Their delays are one millisecond and perhaps even less.

While Hollywood would like us to think that robots and drones and artificial intelligence will one day replace humans entirely, that's not likely to happen. It still takes humans to react to the unexpected on the ground or in the air.

YOUR POWER COMPANY IS SPYING ON YOU

You aren't just being watched online. You're being watched offline—especially if you're trying to go off the grid. Across America, individuals who have decided to start growing hydroponic vegetables, like tomatoes, lettuce, strawberries and squash, are stunned to find themselves at the business end of a dozen automatic weapons being wielded by police and SWAT (Special Weapons And Tactics teams). According to various court cases, those individuals can thank their local power companies for that.

Although it's considered "urban legend," by many, the fact is power companies can and do notice surges in power use, or frequently tripped circuits due to excessive power use and they will contact law enforcement with their concerns. They know that an increase in power use is usually a sign a customer is up to something illegal, like growing pot or cooking meth, although it can often mean someone has just started growing tomatoes or started an aquaponics operation and is now growing fish and/or veggies and not necessarily marijuana or illegal plants.

Either way, if you're considering starting a growing operation of any kind, or are increasing your use of electricity because of a new business or hobby, be aware that it could lead to additional surveillance by your power company or your local police.

KEYWORD LOGGERS

It's easier than ever for someone to install a keyword logger on your computer without your knowledge or consent. Keyword loggers are software programs that track and record keystrokes, clipboard activity, and Net surfing on individual PCs or networks (with administrative access) without users being able to see it or disable it.

If someone has access to your computer, even for just five minutes or less, they can download and install a free Keylogger program. So why would someone do that? If you're a parent with kids, or a suspicious spouse, or a business owner, it only makes sense

you might want to know what your kids or employees are doing on your computer.

There are legal and ethical reasons people would install a keylogger, but there are unethical reasons why someone would want access to see what you're doing online, or even offline. Passwords, letters, files and emails, anything you type becomes visible to a person with a logging program. The best way to keep from having a program installed on your computer is not to share your computer.

It's virtually impossible to tell if you have a keylogging program installed on your computer once it's there. While most keyloggers are after credit card and other financial information, there are many keyloggers who use the software as part of industrial espionage efforts on a global or national scale. Losses to businesses and individuals range in the millions of dollars every year.

A report issued by Symantec shows that almost 50% of malicious programs detected by their analysts are used by cyber criminals to harvest personal user data. According to research conducted by John Bambenek, an analyst at the SANS Institute, approximately 10 million computers in the US alone are currently infected with a malicious program which has a keylogging function.

How do you protect yourself from keyloggers? Learn how these programs can be installed and beware. According to Securelist.com, keyloggers are installed in various ways:

- ✓ a keylogger can be installed when a user opens a file attached to an email;
- ✓ a keylogger can be installed when a file is launched from an open-access directory on a P2P network;
- ✓ a keylogger can be installed via a web page script which exploits a browser vulnerability. The program will automatically be launched when a user visits an infected site;
- ✓ a keylogger can be installed by another malicious program already present on the victim machine, if the program is capable of downloading and installing other malware to the system.

Keyloggers are one form of attack that can let hackers, government types, phishers and scammers gain access to your private information, but viruses are another way people can find their way into your computer.

A computer virus is a piece of software or code that runs on your computer and does different things to your computer without your knowledge or consent. Some viruses are simple, allowing ads to appear, or popping up pictures or an audio or photo file that is annoying. Others are more

malicious, doing everything from erasing all the information on your hard drive, to corrupting, changing or locking down your information so you can't access it.

Some viruses can steal your information and email it to the hacker, or just replicate itself and email the virus to everyone in your contact list. Getting, installing and using the best anti-virus software possible is important.

Be aware that free anti-virus software is often a trojan, or actual virus itself. Better to pay for a recognized, certified malware, virus free program like Webroot, or Norton than to download a free antivirus software. If you can't afford antivirus software and must rely on free versions, try these:

http://www.malwarebytes.org for PCs. You must manually update it and

http://www.avast.com/index for both PC and Mac operating systems

http://avira.com for both PC and Mac operating systems

VIRUSES

The first thing most of us do when our computer stops working, or starts behaving differently is assume we have a computer virus. However, 99% of the time our computer glitch is a computer problem, not a virus. A virus is a small program written to alter the way a computer operates, **without the permission or knowledge of the user**. A virus must meet two criteria:

It must execute itself. It often places its own code in the path of execution of another program.

It must replicate itself. For example, it may replace other executable files with a copy of the virus infected file. Viruses can infect desktop computers and network servers alike. If you truly have a virus chances are it's sending itself to your friends and contact or email list.

Malware is more likely to be what's infecting your computer. Malware includes computer viruses, computer worms, Trojan horses, most rootkits, spyware, dishonest adware and other malicious and unwanted software, including true viruses.

A true virus may or may not make itself noticeable. It may run silently in the background until the user or anti-viral software discovers it, or it may simply replicate itself and infect other computers. It may be timed to go off or shut down or destroy your files on a certain date or when you perform certain functions or visit a certain website.

Worms and Trojan horses. Worms and Trojan horses, which are technically different than viruses, can be worse than a virus. Worms can exploit your security vulnerabilities and spread themselves automatically

to other computers through networks. Worms are programs that replicate themselves from system to system **without the use of a host file**.

Perhaps most unnerving are Trojan horses—a program named after the legendary story of how the Greek army entered Troy, hidden in a oversized wooden horse that hid soldiers inside its belly. The horse, with soldiers inside, was brought inside the gates of Troy. While the city celebrated the soldiers snuck out and killed the soldiers.

A Trojan program does much the same thing. It appears harmless but hides malicious functions that come out after you've loaded and activated the software program, game or download on your device—thinking it to be harmless. Worms and Trojan horses, like viruses, may harm a computer system's data or performance, slow it down, make it run poorly or erratically or be worse—erasing all your files or destroying or corrupting your data.

MALVERTISING

Mal-ware is short for malicious software. Like a virus, it is designed to disrupt your computer's operation, to steal financial information, or to access your private information. New gadets, new apps and even new computers may come already infected with malware! The Department of Homeland Security says that a lot of software and digital gadgets coming into the country is arriving with malware already embedded.

Many of the components installed in computers from the manufacturers from other countries are created with security risks. The Department of Homeland Security won't be specific or name names, but they do say that components in brand new devices are arriving in the USA with malware installed. Buyer beware.

Rootkits. Rootkits are perhaps the worst possible malicious software you can have. They're hard or impossible to find, but can cause the most damage. Rootkits are stealthy software designed to hide their existence and the kind of process they're launching.

Once a hacker or attacker has administrator access to your computer (another reason for never going online using an administrator account) they can install the rootkit. Once installed it's possible to hide both the intrusion as well as the access since the key is the root/Administrator access.

The phisher, hacker or user not has full control over your system, meaning that they can now change existing software or modify any software you might use to detect the rootkit or delete it. Rootkits can often only be eliminated by wiping and re-installing the operating system, or resorting to replacing your hardware (hard drive).

PORNOGRAPHY

For millions of Americans, pornography is very, very addicting. But it's more than just a guilty pleasure, it's the number one source for malware, viruses and trojan software in the world.

Computer experts say that because free pornography is such a draw to millions of men, many of them with families, jobs and credit cards, that malware, keyloggers and trojan software (malicious software hidden inside other programs, like porn videos and photos and files) are rampant. If you are looking at free porn sites, chances are you're being infected with some sort of computer virus while you're there.

While you'd like to think that you're anonymous on a porn site, you're probably at the greatest risk of all. People who have their identities and credit cards stolen or compromised on these sites are most likely to be unwilling to report the loss of their card immediately for fear of humiliation or embarrassment too.

PHOTOS

Photo sites of all kinds can also be a risk. If you're downloading photos from YouTube, or clicking on links or sites you don't know, your risk of downloading a virus or keylogger increases as well.

ENCRYPTION

Child pornographers, the mafia and cheating spouses have already discovered that the last place to find privacy online is through encrypting the files, photos and information they don't want anyone else, including the police or law enforcement from any sector, to access. However, if you are stopped, whether at an airport, by the police, or anywhere you may be with a computer and some encrypted files of legal or illegal contents, you'll have to either give up your password or give up your computer[4].

According to emagined.com, the government may seize your computer and keep it for an indeterminate period of time while they examine it for contraband. Apparently, after a recent ruling by the United States District Court, you have essentially no rights in this matter. [Genao v. U.S., 2009 WL 1033384 (U.S. District Court for the Southern District of New York 2009)] This is true even if you are a US citizen with a valid passport having traveled abroad legally and satisfied all of the procedural requirements.

The government need not show "probable cause" in order to look at your computer. In fact, as with compulsory sobriety checkpoints, the government may simply pursue a program of spot checks and random searches in order to reach its

reasonable goal of preventing contraband from entering the country.

The real legal issue here is, of course, the presumption — now recognized by the United States government judicial system — that any use of encryption (a) is a reasonable indicator that the encrypted material contains evidence of criminal activity or contraband and, (b) that the burden of proof transfers to the claimant to prove that the encrypted files do not contain evidence of criminal activity or contraband. Since it is already established law that under the Fifth Amendment, one cannot be compelled to reveal a password, it now appears clear that a prudent, law-abiding citizen has no option but to surrender his or her laptop upon demand by the Customs Service.

Bottom line? If you don't want the government having access to your computer or your computer files, don't travel with a laptop or other device that has your files on them.

Realize that even if you do encrypt your files that Microsoft Corporation has been working hand-in-hand with the National Security Agency (NSA) to help them bypass encryption technology.

That information was released in 2013 by Edward Snowden, a 30-year-old former systems administrator for NSA contractor Booz Allen Hamilton. Snowden provided the British newspaper, The Guardian, with files detailing a sophisticated relationship between America's intelligence sector and Silicon Valley which included Microsoft's working with government agencies to violate American's privacy.

According to various media reports Microsoft didn't just cooperate with the government, but went out of their way to help them violate American privacy.

PRETTY GOOD PRIVACY (PGP)

The most common form of email encryption is Pretty Good Privacy (PGP). You and anyone who you want receiving secured and encrypted email must have PGP compatible software installed and have the sender's encryption key for it to work.

Think of PGP as a code, which it essentially is. PGP encrypts your email before sending it. If the email or document or whatever you've encrypted is intercepted at any point between your computer (or where the file was sent from) and the destination computer, it is impossible to read. Some email providers also offer Transport Layer Security or Secure Sockets Layer encryption.

It's the most secure method of protecting your privacy, although if the government wants to see what you're sending, they can put their code

breakers on it (although it's not likely unless you're suspected of encrypting some pretty important stuff).

VIACRYPT PGP

ViaCrypt PGP is a commercial public-key encryption package which is based on, and virtually identical to, the freeware program known as PGP, or "Pretty Good Privacy".

http://www.gamers.org/~tony/pgp-legal.html

http://security.stackexchange.com/questions/24783/how-effectively-can-isps-detect-illegal-file-sharing

10 BEST PRACTICES FOR CREATING A SECURE HOME NETWORK

Use the latest, greatest software and Operating System for your computer. Windows 7 and Vista are better than XP. Update your software and operating system regularly (daily or weekly). It takes only minutes to update your system, so get in the habit of doing it. Use Microsoft Office 2007 or later as its XML formats for storing files protect you from computer files that execute embedded codes when opened. The Office 2010 suite of Microsoft products also provides a "protected view" option which lets you open documents in "read only" view to help minimize the impact of malicious files.

If you don't want to manually update it, then go into your preferences section and configure your system to provide updates automatically. All systems give you the option of checking for updates automatically, then alerting you to the fact they are ready to install, leaving the update to you.

Install a comprehensive, host-based security program and make sure you install updates as they become available. Get a program or suite of programs that protect you against viruses, and phishing. It should provide a safe browsing system with firewall capabilities. It should also provide a Host-based Intrusion Prevention System (HIPS).

Check with your Internet Service Provider (ISP) as many of them offer such services free or at a small additional monthly cost. If you're on a Mac, make sure you update your iPad, and any other Apple devices by syncing them at least once a month, or prior to traveling anywhere you plant to use your laptop, iPad or other device. If you have third party applications for things like video, accounting etc. make sure they're also updated regularly.

1. Limit the use of your computer's administrator account. Most users create an administrator account, then use that account to do everything—from browsing to adding software to reading email. That's a bad idea.

Create the administrator account, then create another account for yourself. Only use the administrator account (the one with the passwords and other information) for installing updates, adding software or reconfiguring the computer if needed. When you're reading email, browsing the web or using an administrator account for anything online you're opening yourself up to being hacked.

2. Use a Web Browser and PDF reader with Sandboxing capabilities. Sandboxing is a term that describes software that keeps applications within a certain framework that keeps them from getting loose on your computer.

Because many PDF files now contain executable files or programs, a PDF reader and web browser that provide sandboxing capabilities block embedded URLS (Website links to malicious sites) by default.

3. Enable Data Protection on Apple Devices. The iPad comes with a data protection feature that protects the hardware encryption keys with a passcode. This feature is available on laptops as well. For more information on this feature: http://support.apple.com/kb/HT4175. Implement FileVault on Mac OS Laptops, and check the Apple website for additional security features your Apple products may have.

4. Protect Your Home Network by configuring your system correctly. If you're not sure how to do that, hire a trusted professional who can. Ask them to:

5. Implement an alternative DNS Provider. The Domain Name Servers (DNS) your ISP provides rarely provide the enhanced security services you need. Commercial DNS providers like

6. Set up your router away from windows and in a central location in your home or business. The less Wi-Fi leakage you have, the less likely someone driving by is likely to see it or hack into it. If you use WiFi infrequently, then turn it on only when you're using it. Many people use a laptop in bed, or tablets or phones and other devices throughout the day and evening. But if you only use WiFi in the evening, then turn it off during the day or when you're away from home.

7. If you have a router (and chances are you do if you use a wireless device such as bluetooth or WiFi in your home), change the administrator passwords that come with the router. Most routers come with a 123456 or blank password and anyone who wants into your system knows it.

Turn on encryption, either WEP, WPA or WPA2 so anyone passing by, or parked on the street, or living next to or above/below you can't access your network without the password.

8. Change the default SSID or name of your network and then disable the SSID broadcast. For instance, if you bought a NetGear or LINKSYS router the default name is going to be NetGear or LINKSYS. So when a hacker or intruder sees your signal, they see LINKSYS or NetGear. Change the name to something very neutral, like a color, then disable the SSID broadcast. Whatever the network name is, you can disable it so people outside the system can't see it.

9. Enable MAC address filtering. This filtering basically tells your router to only let certain devices you designate on your network.

10. Finally, do not auto-connect to open Wi-Fi networks, including those at coffee shops, McDonalds, or any you find when out in public. When you just connect to open Wi-Fi networks, you're also exposing yourself to any risk or danger coming from those networks.

SECURE AND UNSECURE WEBSITES

HTTPS stands for "Hypertext Transfer Protocol Secure. HTTPS is a combination of the Hypertext Transfer Protocol (HTTP) with the Secure Socket Layer (SSL)/Transport Layer Security (TLS) protocol. TLS is an authentication and security protocol widely implemented in browsers and Web servers. SSL works by using a public key to encrypt data transferred over the SSL connection.

Most Web browsers support SSL. It allows you to communicate securely with the web server without fear that a third party can read or see the information you are transmitting, such as a banking transaction or charge. Sites that have HTTPS are more secure than sites without it, but there is still no guarantee an HTTPS site is legitimate or safe. Professional Internet thieves know how to make a site look very legitimate!

PUBLIC AND/OR UNSECURED WIFI

Hackers can join any unsecured Wi-Fi hotspot easily stealing your user information and taking control of your accounts. If you simply can't resist the urge to check your email or do other things online (Facebook, Twitter, etc) while using public WiFi you're risking having your identity stolen.

Most wireless routers can encrypt transmissions. However, if the encryption is disabled, anyone within range of the router can use monitoring software to intercept and read transmissions. The reason you want to enable your router's encryption feature and put a secret key on every connected computer in your home so to keep intruders from connecting to

your network or viewing the information you send over the Internet.

SOCIAL MEDIA

Facebook and other social media sites like LinkedIn, MySpace, and so on are full of friendly, helpful people. But they're not all they appear to be. Just because the Internet feels safe doesn't mean it is. What you think is someone being friendly and nice could be a new friend, or it could be a criminal using social engineering (the use of standard friend making practices) to gain your trust and access to your personal information.

Only time will tell. Most criminals are looking for a fast, easy score and will rarely spend the time to gain your trust. Pedophiles however will take their time, spending weeks, months and even years to lure your child into a relationship where they trust the person enough to meet them offline. So be extra vigilant about your personal information on social media sites.

Not everyone is who they claim to be. If someone you know offline introduces you to one of their online friends, ask them if they've met this person offline or know them personally. They may unwittingly introduce you and create a false sense of safety or trust because you trust your friend.

BEWARE OF ONLINE SURVEYS, POLLS OR QUESTIONS

Getting to know someone often legitimately means getting to know things about them, like their favorite color, their favorite food, and their children or pet's names. Those are often all things people include when creating passwords for their accounts, or as "secret question" answers. If you belong to a group that uses polls and surveys keep in mind that the questions can be more than innocent curiosity.

If in doubt, simply refuse to answer, or make up an answer. There is no law that says you have to use your real maiden name, or your mothers real maiden name on a website. That's just to make it easier for you to remember. It also makes it easier for a phisher to find out the answer by joining a social media group.

The reason people answer these surveys is because they assume a survey or poll is legitimate. They're more willing to answer because they trust that the survey or poll is being conducted for legitimate reasons. It's often not.

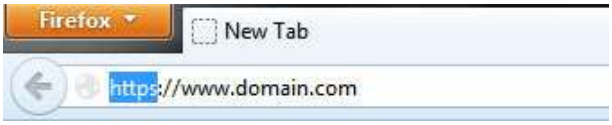
For instance, during the last US Census in 2010 (where the government surveys citizens to determine all kinds of personal information) scammers were out taking advantage of the

public's ignorance about the survey. They used the opportunity to find out personal information as well, relying on the assumption that most survey takers would assume the survey was online.

The fact is, the US Census is a paper and pencil survey only. Very few parts of it were conducted online, and the parts that were did not ask about personal information, credit cards or social security numbers. Still, scammers were still able to social engineer scams that got people to give up personal information anyway. They had people go online believing they were dealing with a safe, secure government site when they weren't.

The sad thing is, even visiting a website like the one in those scams, even to see if it was legitimate could result in triggering a drive-by virus download. Be very wary of any online communications—including emails and social networking messages—that you receive regarding the census. If you're asked to click on a link or URL, open an attachment or respond with personal information, chances are you're downloading a virus. Many of today's malware infections occur when a user simply visits a malicious or compromised website.

Just because a company has a great website doesn't mean it's a secure site. Millions of small to medium sized businesses either can't afford, or simply don't want to pay the high prices to ensure their site is secure for online transactions. It's up to you to determine, or look for the clues that tell you a site is secure. The most easily recognized sign a website is secure, or that your financial information is encrypted and unable to be read by anyone is HTTPS:// in the web browser.



HTTPS

The "s" on the end of "http" in your browser window is what tells you the website you're on is secure. If you see "https" in the web address window of your browser it means the session between the web server and the browser on the computer or mobile device you are using is encrypted. https://www.paypal.com is one such site. Your bank, electric company or other large company you regularly do business with online is likely to have an https:// designation.

HTTPS stands for "Hypertext Transfer Protocol Secure. HTTPS is a combination of the Hypertext Transfer Protocol (HTTP) with the Secure Socket Layer (SSL)/Transport Layer Security (TLS) protocol. TLS is an authentication and security protocol widely implemented in browsers and

Web servers. SSL works by using a public key to encrypt data transferred over the SSL connection. Most Web browsers support SSL. It allows you to communicate securely with the web server without fear that a third party can read or see the information you are transmitting, such as a banking transaction or charge.

Don't just assume that because you see the icons, banners and even the https:// designation that the site is legitimate. Criminals, phishers and thieves can make their scam sites look more legitimate than the real sites. So look for the https:// and the Verisign and other logos, but more importantly only do business with websites that you know and trust. If you find a new site with great deals, search on their name and the words "scam" or "phish" to see if other users have reported problems with the site. If in doubt use a service like Paypal or a prepaid debit card.

PUBLIC PLACES WITH PUBLIC WIFI

If you travel for work, or school, or simply like to work outside the office, you probably rely on free public WiFi to access the Internet.

Places where you may encounter unsecured WiFi

- ✓ Fast food restaurants
- ✓ Coffee Shops
- ✓ Truck Stops
- ✓ Libraries
- ✓ Hospitals
- ✓ Schools (including high schools, universities, community colleges etc)
- ✓ Using someone else's WiFi (neighbor or business)
- ✓ Gyms
- ✓ Bookstores
- ✓ Hotels or motels
- ✓ Community WiFi

These places are wonderfully convenient, but wonderfully dangerous as well. With unsecured WiFi anyone can discover and steal your login information using an extension in their Firefox browser called "Firesheep."

Firesheep intercepts unencrypted cookies from various websites and allows that person to steal your login information, read your email and access any web page you're reading at the time. It's not the only software capable of intercepting your information. You're fairly well

protected from hackers and thieves when using major websites, but you're still at risk.

If you must use public WiFi do not conduct banking, business or any other sensitive transactions online. Limit your use to surfing and activities that don't require logging into any accounts.

Some sites, like Facebook, Google, PayPal and Twitter use something called always on SSL, meaning all its pages are encrypted and secured. Facebook now uses HTTPS for all its users. They also require all apps on its platform to use HTTPS with an SSL certificate from a trusted Certificate Authority. These sites are safer, but not totally safe. If at all possible, wait until you're home or on a secured connection to login to any account.

Google built many of their applications with HTTPS support from the very beginning, and has made HTTPS the default setting for users who are logged into their Google accounts, even for search queries.

Twitter gives its users the option to always use HTTPS, and also uses the t.co service to protect hyperlinks from being hijacked. PayPal implemented site-wide HTTPS many years ago, as well as HSTS so that their website will only accept HTTPS connections.

PROTECT YOUR PRIVACY OFFLINE

Just because you're not online, on a computer or using a cellphone doesn't mean your privacy is protected. If you use a bank card, credit card, debit card, passport, employee ID or school ID chances are your card has an RFID chip in it that allows your school, employer or issuing agency to track your movements, spending and shopping habits. If you want to stop or eliminate that, keep your cards in an RFID secure wallet.

RFID stands for Radio Frequency Identification. RFID chips are smaller than a grain of rice. Indeed, they are small enough to fit into a hypodermic needle where they can be embedded into your skin, or into your pet's skin to help authorities track you better. This can happen with or without your consent, such as when receiving a flu shot, vaccination or other medical procedure.

Some hospitals or doctors may suggest you consider being chipped, or having a family member (child, senior adult) chipped as a way to ensure easy access to your medical records in an emergency. Even if you decline being chipped, you may not have a choice when it comes to your financial and property rights. Many new tires come automatically chipped with RFID devices. This allows toll road devices, rest stops and other monitoring stations to record your tires when you roll by. Cars manufactured after a certain date also contain RFID chips as do televisions, monitors and other items. If you're not sure if something is chipped, ask.

Credit card companies and banks embed RFID chips into their cards so vendors can scan your credit or debit card more quickly. Not all cards are vulnerable, but most are. How can you tell if your cards are "contactless cards" and RFID readable?

Take your cards out of your wallet and flip them over. If the back of your MasterCard says "PayPass," or your Discover Card says, "Zip" or your American Express card has the words, "Express Pay," on it, you're vulnerable. There are currently more than 100 million of these contactless cards in circulation.

Of course your credit card company doesn't want you to know it, and the payment cards industry has repeatedly denied that their cards are easily read and information stolen, but year after year at hacker's conferences around the world, hackers demonstrate just how easy it is to read, steal and get away with wireless pickpocketing.[1]

If you have a gasoline card that you wave over a sensor at a gas pump the RFID chip inside is telling the machine you are a verified card holder, or it gives the machine the go ahead to charge your card without your having to swipe it through a card reader.

If you travel, authorities at border crossings and airports use RFID readers to scan your passport at a difference. This makes getting through security faster, but it also allows officials to scan your information if they think you're acting suspiciously for any reason. If you've had an argument with someone, are tired, stressed, or simply lost you may exhibit behaviors police or airport or transportation authorities consider suspicious.

With a reader they can scan your wallet, your passport and your driver's license and get all the information they want in order to make a decision about whether to detain you for questioning or not, and you never even know they've been watching you.

Law enforcement officials aren't the only ones with access to RFID readers. Criminals have them too. They can sit in a crowded airport, bus station or subway station and collect anyone, or

everyone's credit card, driver's license and other ID without their victim's ever knowing they've been scanned.

Using an RFID blocking wallet will stop anyone with a reader from accessing your information. RFID blocking wallets come in all shapes and sizes for credit cards, passports and identity cards. They may be made of leather, a special fabric, metal, or other blocking material, but they're all designed to do one thing—stop RFID readers. Once you are ready to make a purchase, or show an official your card or ID you simply slip the card out of the wallet and scan it. There's a risk of being read by another reader as you do this, but it's less likely.

RFID readers, depending on the kind of reader and the quality, can scan and read information from a credit card as far away as three feet. Your crook doesn't have to be rich or smart to steal your ID this way. RFID readers can be purchased for as little as $50 to $100, and the technology to turn your name, card number and identity into someone else's shopping spree within minutes doesn't cost much more, about $200 to $300.

If you're really concerned, keep an eye out for a soon to be on the market RFID signal jammer called GuardBunny. GuardBunny looks like a typical RFID blocker, except the GuardBunny logo (a bunny) has eyes that glow when it detects a reader nearby (legit or illegitimate reader). And instead of just blocking the reader, it actually jams the electromagnetic signal of even the most powerful readers made.

IDENTITY THEFT

Your chances of having your identity stolen are one in five. That's how many people report having their identity stolen every year. What is identity theft? It's when someone steals your personal information and uses it without your permission. While most of us assume someone has to steal your social security number to steal your identity, that's not true.

They can steal your passport, your driver's license, your birth certificate, even your bills in order to create a fake identity. In fact, one of the requested forms of ID many companies (electric, phone, car rental etc) request is a copy of a bill with your name and address on it.

THE 6 PEOPLE MOST LIKELY TO STEAL YOUR IDENTITY

1. Family members (mother, father, siblings, spouse, foster parents)
2. Waiters and waitresses or bartenders
3. Store Clerks
4. Catalog companies
5. Fake websites
6. Professional Identity thieves
7. The US Postal Service

(1) FAMILY MEMBERS

Sadly enough it's your nearest and dearest who are most likely to steal your identity, as well as your cash, checks and other assets. Not only do they have access to your credit cards, social security number, employee ID's and other information, they also have your trust. They're also the people you're least likely to suspect.

Love your family, but protect your personal banking, social security and credit information as well as your checkbook. When you balance your checkbook each month take time to go through your checks and make sure none are missing. Keep your checks locked up. Your family may be trustworthy, but their friends and acquaintances may not be. If you entertain frequently, make sure any personal information, checks, papers and files are securely locked up.

If you have teen-agers stress the importance of privacy and identity theft and the need to protect their own identity from friends. Children are trusting, but statistics show that teenagers will steal from their own friends and family.

CHILD IDENTITY THEFT

Child Identity theft, which is someone stealing your child's social security or ID, is at such extreme levels that the US Department of Justice holds seminars to help law enforcement personnel learn how to investigate, stop and prosecute it.

There are many signs that should tip you off to the fact that someone is misusing your child's personal information and committing fraud:

» You or your child may be turned down for government benefits because the benefits are being paid to another account using your child's Social Security number

» You may get a notice from the IRS saying the child didn't pay income taxes, or that the child's Social Security number was used on another tax return

» Get collection calls or bills for products or services you didn't receive

» Be the subject of an IRS audit or investigation

WHEN TO SUSPECT CHILD IDENTITY THEFT MAY BE A POSSIBILITY

» Child service providers ask for or require your child's Social Security Number when signing you up for service

» You're in the middle of a divorce or child custody battle

» Your spouse, ex-spouse or family member is having financial difficulties

» Your spouse, ex-spouse or family member has addiction or alcohol issues

HOW TO PREVENT CHILD IDENTITY THEFT

Never share your child's Social Security number unless you know and trust the person asking for it. Keep your child's Social Security Card locked up or in a safety deposit box. If someone such as a school, teacher, service provider etc. asks for the number don't just automatically give it to them.

Ask them why it's necessary and how it will be protected. Also get the name (first and last) of the person requesting the number. Ask if you can use a different identifier, or use only the last four digits of your child's Social Security number, or use your number instead.

Notify your child's school in writing that, pursuant to the Family Educational Rights and Privacy Act (FERPA)[2] that you do NOT want your child's information released without your knowledge or consent. Schools may disclose, without your consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. This is all information an identity thief could use.

However, according to the Act, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification, in other words HOW the school notifies you (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.

For more information about FERPA visit http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

HOW TO FIND OUT IF YOUR CHILD IS A VICTIM OF CHILD IDENTITY THEFT

Contact each of the three nationwide credit reporting agencies:

1. Experian
2. Transunion
3. Equifax

Request a manual search of the child's file. The companies will check for files relating to the child's name and Social Security number, and for files related only to the child's Social Security number. The credit reporting companies may require copies of:

» the child's birth certificate listing parents

» the child's Social Security card

» the parent or guardian's government-issued identification card, like a driver's license or military identification, or copies of documents proving the adult is the child's legal guardian

» proof of address, like a utility bill, or credit card or insurance statement

(2) WAITRESSES AND WAITERS

It's nice to be able to put your meals on a credit card and not have to worry about cash, but you increase your risk of credit card theft, unauthorized purchases and identity theft each time you do. Not all waiters and waitresses are out to hit your cards, but it happens more frequently than you'd guess.

In 2011 seven waiters were arrested in NYC as part of a credit card theft ring.[10]

The thieves, all waiters in high-priced steak houses, were using hand held scanners to capture credit card information from high credit limit cards, then sending the information to credit card ringleaders who created new credit cards with the information.

If your server is taking a long time with your credit card, or disappears into the back of the restaurant instead of heading towards the cash register or checkout station, make sure to contact your bank or card company as soon as possible and inquire about any charges. Better yet, sign up for notification or a text message that goes to your cellphone every time you make a purchase. The text message is a confimation of legitimate purchases and an early warning for illegitimate ones. Most text messages alerts are free, or cost only the fee your

cellphone provider charges—a small price to pay for peace of mind.

(3) STORE CLERKS

Clerks, like anyone else who handles money, cash or credit, have the opportunity to capture your card numbers and information and steal it or sell it to someone who then creates a new identity or simply runs up your card limit. When shopping pay attention to the clerk handling your transactions.

Don't talk to your friends, or on your cellphone while the store clerk has your credit card. Don't hand the card to the employee until all your transactions have been entered and rung up on the cash register. Then watch your card until it's back in your hands again. If the clerk must leave the register, request your card back. There's no reason a clerk needs to leave their register with your credit card. It takes only seconds for a clerk to go to a back room, swipe your card or take a photo of it with their cell phone and send your information to someone.

Don't let it happen. If your card is in someone else's hands, watch it until its back in yours. Most businesses require you to swipe or punch in your information yourself. All the better. If a clerk asks you for the security code on the back, show it to them, don't read it or say it out loud. It's too easy for another customer to hear it, and if that other customer happens to be a criminal, it's easy for them to see, hear or write down your card information if they really want it.

Many criminals use cameras built into their hats, purses or even pens to capture your card number. Never hold or pull your credit card out until you're ready to use it and keep the numbers covered.

(4) HOW CATALOG COMPANY EMPLOYEES CAN STEAL YOUR ID

If you've ever ordered from a catalog company, chances are you've used a credit card. And if you've used a credit card you've heard the sales clerk on the other end of the line repeat your name, address and information back to you, right? They want to make sure they have your correct information. There's nothing wrong with that!

The problem is many of these companies have a tremendous employee turnover and not every one they hire is honest or ethical. Their customer service representatives are often paid minimum wage to do a high stress job. Some get a quick background check, or a credit check to ensure they're not an obvious security risk, but many do not.

These are the agents who eavesdrop and listen for their co-workers to read back your credit card information. They write it down and give it or sell it to identity thieves. The source of the theft is sometimes never discovered. Never ever let anyone repeat your credit card information aloud, and never give out your credit card information over the phone within hearing distance of anyone. If possible, punch in the numbers of your card on the phone rather than speak them.

If you can possibly avoid ordering anything online or in public via your cellphone or texting, do so. Criminals hang out in bars, restaurants, malls, in check-out lines and banks just hoping or trying to get credit card numbers, names, information or account details. They use cameras, binoculars and digital devices to swipe your card info. They can use RFID readers, or a number of technologies to steal your financial or personal data without your ever knowing you've been robbed or scammed.

So pay cash as much as possible and keep your credit, debit and other cards, or passports inside an RFID proof wallet or protective sleeve. Paying cash not only helps you protect your identity, it doesn't leave a paper trail of purchases or give stores or others ways to profile you.

When you do order online, even from the privacy of your home, ask the clerk or customer service rep to let you read your credit information back to them rather than have them repeat it out loud to you. If they say it's policy to read it aloud explain your concerns about theft and most will understand and honor your request. If they don't, ask to speak with a supervisor.

You may still get a crooked clerk, but since all transactions are recorded and monitored they're much less likely to steal your identity if it can be traced back to them. If someone hears them and writes the numbers and info down, they're a victim too. Since most companies record all calls you have a record (If you write down the date and time of your call) and proof that you expressed concern over theft. That goes a long way towards getting a company to settle with you rather than have you report that on social media.

PREVENTION

Buying things online is convenient and easy, until your card number gets stolen. Whenever possible use pre-paid debit cards, PayPal, or gift cards rather than a credit card. Load the prepaid cards only when you want to make online purchases, or limit your total amount of cash on the card to a number you could afford to lose if it were stolen. Remember to always use your bank debit and prepaid debit cards as a "credit card" on any store or bank purchases rather than as a debit card.

This protects you against any bad purchase, or in the event you want to return an item, and it keeps criminals from capturing your punching in your PIN number as well. If you must use your PIN number for a transaction, block the view of the pad from others. Don't worry about offending others around you. Honest people will think nothing of it and who cares if criminals are frustrated.

(5) FAKE WEBSITES

Fake websites are an online threat, but they are also one of the top six ways people can steal your identity, so they're listed here in offline privacy. Even if you aren't online, you may have friends, relatives, employers and neighbors who are online and who may use your name and information to set you up on a dating website, or share your information in ways they think are being helpful, like sweepstakes or contests.

Not all websites are what they appear to be. Many are set up by scammers and phishers intent on one thing—getting your information so they can drain your bank account, steal your identity or max out your credit cards.

Before entering any personal information into a new website go to http://duckduckgo.com (a search engine that doesn't track your websearches) and search on the name and investigate them.

Do they have a street address? Google Earth search it to see what their brick and mortar store looks like and if the store has the same name as the website. Spending 20-30 minutes checking phone numbers, Yelp, Google Earth and independent reviews can save you a lot of headaches down the road.

Does the company have a variety of reviews? How long have they had a website? Who answers the phone when you call? Or does it go to voicemail? If in doubt, leave the site and don't enter your information.

Using a service like PayPal disguises your financial information and protects your online purchases. PayPal accounts are free to set up and use. You can even request a PayPal debit card that allows to you access your money, add money or buy and sell online without worrying about your identity or financial information being compromised.

(6) PROFESSIONAL IDENTITY THIEVES

Some people prefer the drug trade, burglary or robbery and still another set of thieves prefer to steal identities. These are smart, savvy professionals who can turn your stolen credit cards into a duplicate personality who then

opens new credit lines, maxes them out, and even gets a new driver's license and proceeds to do all sorts of mischief, while pretending to be you. It can get really ugly.

Someone who is determined to get your information or who targets you specifically, probably has the expertise, technology and resources to get what they want. The chances that someone like that is targeting you is very, very remote, and if they are, they're so good you won't be able to stop them.

What you can stop are the opportunistic criminals, the ones who see you are lax in your protection, or who happen upon you when you're not paying attention, or you've gotten lazy is protecting your wallet, information or credit. They may be a stranger you've friended on Facebook or a social media site. They may be someone you've met on a dating site, or someone in your community pretending to be someone else online.

The best you can do against a professional is to be aware and prepared and hope that alone diverts their attention to someone else. Professionals look for easy marks and if you make it hard, they're going to go elsewhere.

HOW TO PROTECT YOUR CREDIT AND DEBIT CARDS

The number one thing people fail to do when they suspect their identity and/or their credit cards have been stolen is to take action immediately to stop the fallout from a stolen ID. Acting fast limits your liability for charges you didn't authorize. Every major company has a toll-free number and 24-hour service for lost or stolen cards. But it's up to you to call that number.

Immediately calling the top three credit bureaus to freeze your account or put a watch on your account when your cards are lost or stolen can shut down a would-be identity thief fast. In fact, having a lock or check with your homeowner's or renter's insurance agent. Your homeowner's or renter's policy usually covers your liability for

card thefts. If it doesn't, ask your agent to do so. Some insurance companies will allow you to change your policy to include this protection if they don't already offer it.

WHAT TO DO IF YOUR IDENTITY IS STOLEN: STOLEN CARDS VERSUS IDENTITY THEFT

Not everyone who steals your credit cards, wallet and ID will open new accounts in your name or ruin your life. Most thieves will just steal your cards and money, use them then throw them away. Others may sell them to someone who deals in stolen cards and be done with it, but the person who buys your stolen card may set out to create more cards with your identity, making it very difficult to stop.

As common criminals have become more Internet savvy many of them will also use those cards and ID to do exactly that— steal your identity. So how do you know if the person who has stolen your credit cards and ID is also out to steal your identity? You don't. So you have to assume the worst if you truly want to protect your credit and your identity. If your cards are stolen act as though your identity has been because chances are, it has.

Once you realize you're a victim of identity theft you need to act fast and act immediately. Contact every financial institution and credit card company where you maintain accounts. In the USA you need to contact each of the three major credit bureaus: Equifax, Experian and Transunion by phone and email.

When you contact the financial institutions and credit card companies you do business with, request that they close your current accounts and issue new credit cards and financial accounts with new card and account numbers. Next, review all your recent transactions and dispute any fraudulent credit card charges or financial account transactions. If you see any monies have been stolen from your accounts, insist that those funds be restored.

By notifying any one of the three major credit bureaus that you are a victim of identity theft or suspect that you are a victim of identity theft, that credit bureau is responsible for notifying the other two credit bureaus on your behalf, but don't wait or assume that will happen. Contact all three. Better to have redundant reporting than no reporting:

The three major credit bureaus can be notified at the following addresses and phone numbers:

Equifax Credit Information Services, Inc

P.O. Box 740241 Atlanta, GA 30374

1-888-766-0008

TransUnion Fraud Victim Assistance Department

P.O. Box 6790 Fullerton, CA 92834

1-800-680-7289

Experian

PO Box 9532 Allen TX, 75013

1-888-397-3742

When you notify the credit bureaus, be certain to request that the credit bureaus place an initial 90 Day Fraud Alert on your credit file. Once a 90 Day Fraud Alert is placed on your credit file with each of the three major credit bureaus, you will be entitled to receive a free credit report from all three of the credit bureaus. Inspect each of the three credit reports closely and determine if there are any credit accounts that have been fraudulently opened in your name.

Inspect the credit report closely for any inaccurate information on legitimate credit accounts contained with the report. Additionally, be sure the information at the top of the credit report containing your name, address, date of birth and social security number is accurate. Be certain that the credit bureaus remove any inaccurate information or fraudulent accounts from your credit reports.

Finally, if you determine that you are in fact a victim of identity theft, you are entitled to place an Extended Fraud Alert on your credit file with each of the three major credit bureaus. An Extended Fraud Alert remains on your credit file for seven years.

You will need to place the Extended Fraud Alert with each of the three major credit bureaus individually. Also, you will need to have a Police Report documenting that you are a victim of identity theft in order to place an Extended Fraud Alert.

Here are the steps you'll need to take:

- ✓ Contact your ATM or debit card issuer.
- ✓ Report the fraudulent transaction. Act as soon as you discover a withdrawal or purchase you didn't make.
- ✓ Write a follow up letter to confirm that you reported the problem.
- ✓ Keep a copy of your letter.
- ✓ Send it by certified mail and ask for a return receipt.
- ✓ Update your files.
- ✓ Record the dates you made calls or sent letters.
- ✓ Keep copies of letters in your files.

Once you report the loss of your ATM or debit card, federal law says you cannot be held liable for unauthorized transfers that occur after that time. That's why it's important to report it

immediately, even if you think you may have just misplaced your card.

It is far less hassle to be inconvenienced and have to get a new card because you've misplaced yours and reported it lost, than to have thieves run your card charges up for a week while you hunt for the card.

Most people fail to act because they have not prepared for this to happen to them. They don't have any idea where to start, who to call or how their life is about to change.

Before you finish reading this book you need to:

1. Empty the contents of your wallet
2. Photocopy both sides of every credit card, bank card, retail charge card and debit card in your wallet
3. Photocopy both sides of your employee ID, your drivers license and all ID pages in your passport
4. Make a list of all the cards you own so you can check off each card after calling the card company
5. Make two copies of all these photocopies and store them in a very safe and secure place—like a safe, or safe deposit box. If your identity is ever stolen you'll need all the numbers on each and every card to report the loss to the company.
6. Write down the phone number of every company on your cards—your bank card, credit card company etc. Go to their website and look for the information they provide "in case your credit card is lost or stolen." Print off everything from the website on what to do if you are a victim of identity theft. Keep that information in a notebook you can easily access.

REPORT IT

Call your local police department FIRST. Until you have an official report filed with the police stating that your card(s), checks, identity were stolen or lost, most companies will simply consider your cards lost and will cancel the cards, but will not stop someone using your identity from opening a new account. They may also refuse to pay any charges the thief racks up on your cards as well.

You must file an official police report claiming IDENTITY THEFT if you discover someone using your cards and stealing your identity. Without an official police report no one will act on your behalf. Get several original copies as the credit bureau may not accept a photocopy.

If you don't already belong to LifeLock.com, considering joining. Plans start at $110 and go up to $275 a year for protection against identity thieves.

Do you need a business or third party's protection? Only if you aren't sure you can handle securing your own information and computer.

WHAT IS A SSN AND WHAT WAS IT ORIGINALLY CREATED FOR?

If you get out your Social Security card and look at it, it clearly states, "Not for Identification Purposes," yet every business and form you encounter asks for it. Just because someone or some business asks for it doesn't mean you have to give it to them. Many clerks and people will insist on having it, only because they were trained or told to ask for it.

When challenged, or when people refuse to give it up, they become angry. That's their problem, not yours. Simply ask them why they need it and demand they provide written proof or documentation of their reason for requiring it. Most businesses use your Social Security solely to run a credit check on you, often without your permission. If you are paying cash, not requesting credit and have no reason to give up your number, don't give it up. You have no way or assurance of privacy or security once you hand over that number to someone.

Many police officers will request your social security number when taking a police report so they can identify you or your case later. What they neglect to tell you is that police reports are public record and anyone can go into a police station and view all the police reports on file at any time and have access to your full legal name, your social security number, phone number, home address and date-of-birth—everything they need to steal your identity, all because a police report of a crime or incident is public record! If officers insist on getting your SSN, insist on giving them an EIN number, driver's license, or other number instead.

An EIN number is free, and takes only minutes to get. There are websites who will charge you anywhere from $19.95 to $400 to get the number for you, but you can get it yourself for free by going to: https://sa2.www4.irs.gov/modiein/individual/index.jsp and completing the form online, or printing it off and completing it offline and then mailing it in to the IRS. It's a simple form and takes about five to ten minutes to complete. The advantage to an EIN is that you can use it, rather than your Social Security number, when buying, selling and conducting business online or off.

You can get an EIN if you:

- ✓ Started a new business (this includes an ebay account, selling anything online via Craigslist, or uploading and selling an ebook etc)

- ✓ Hired or will hire employees, including household employees
- ✓ Opened a bank account that requires an EIN for banking purposes
- ✓ Changed the legal character or ownership of your organization (for example, you incorporate a sole proprietorship or form a partnership)
- ✓ Purchased a going business
- ✓ Created a trust
- ✓ Created a pension plan as a plan administrator
- ✓ Are a foreign person and need an EIN to comply with IRS withholding regulations
- ✓ Are a withholding agent for taxes on non-wage income paid to an alien (such as an individual, a corporation, or a partnership)
- ✓ Are a state or local agency
- ✓ Are a federal government unit or agency
- ✓ Formed a corporation
- ✓ Formed a partnership
- ✓ Administer an estate formed as a result of a person's death
- ✓ Represent an estate that operates a business after the owner's death.

Banks and SSN (By law your SSN can not be used for ID purposes, although everyone uses or attempts to use it for that purpose) . According to the IRS and the Social Security Administration you do not have to give your Social Security number to anyone who asks. Indeed, you should refuse to give it just because someone asks for it. By law, these are the ONLY places you must give your number to if you want service:

The Social Security number was originally devised to keep an accurate record of each individual's earnings, and to subsequently monitor benefits paid under the Social Security program. However, use of the Social Security number as a general identifier has grown to the point where it is the most commonly used and convenient identifier for all types of record-keeping systems in the United States.

Specific laws require a person to provide his or her Social Security number for certain purposes. While we cannot give you a comprehensive list of all situations where a Social Security number might be required or requested, a Social Security number is required or requested by the following organizations:

- ✓ Internal Revenue Service for tax returns and federal loans;
- ✓ Employers for wage and tax reporting purposes;

- ✓ Employers enrolled in E-Verify;
- ✓ States for the school lunch program;
- ✓ Banks for monetary transactions;
- ✓ Veterans Administration as a hospital admission number;
- ✓ Department of Labor for workers' compensation;
- ✓ Department of Education for Student Loans;
- ✓ States to administer any tax, general public assistance, motor vehicle or drivers license law within its jurisdiction;
- ✓ States for child support enforcement;
- ✓ States for commercial drivers' licenses;
- ✓ States for Food Stamps;
- ✓ States for Medicaid;
- ✓ States for Unemployment Compensation;
- ✓ States for Temporary Assistance to Needy Families; or
- ✓ U.S. Treasury for U.S. Savings Bonds

The Privacy Act regulates the use of Social Security numbers by government agencies. When a federal, state, or local government agency asks an individual to disclose his or her Social Security number, the Privacy Act requires the agency to inform the person of the following: the statutory or other authority for requesting the information; whether disclosure is mandatory or voluntary; what uses will be made of the information; and the consequences, if any, of failure to provide the information.

If a business or other enterprise asks you for your Social Security number, you can refuse to give it. However, that may mean doing without the purchase or service for which your number was requested. For example, utility companies and other services ask for a Social Security number, but do not need it; they can do a credit check or identify the person in their records by alternative means.

Giving your Social Security number is voluntary, even when you are asked for the number directly. If requested, you should ask why your Social Security number is needed, how your number will be used, what law requires you to give your number and what the consequences are if you refuse. The answers to these questions can help you decide if you want to give your Social Security number. The decision is yours.

Banks, day care providers, any and all businesses may ask for it, but that doesn't mean they need it or have a right to it. You don't know who has access to your number once you fill in

the forms, so think twice. Pay cash or in full at time of service. Doctors do NOT need your SSN unless you're paying on credit, or a payment plan, yet they routinely ask for the number as do hundreds of other people.

Protect your credit and your privacy when buying a car. Do NOT give your SSN or have any car dealer run your credit history. You give up far too much privacy by giving them your SSN.

PROTECTING YOUR PRIVACY OFFLINE

Okay, so you don't even own a computer or a smartphone. There's no way you're in the system or on anyone's radar, or is there?

Do you have a driver's license?

Do you own property, like land, a car, a boat?

Do you have a Social Security number?

A credit card?

Have you ever gotten a speeding ticket or been in trouble with the law, even as a juvenile?

Have you ever gone to the hospital, emergency room, been in a wreck, seen a doctor, applied for a job, gone to the dentist or attended public or private school?

Do you have credit, even bad credit?

Have you ever flown?

Taken a bus?

Filled out a "buyer loyalty" tag at your local grocery store?

Do you belong to SAM'S club or any buying club?

Have you ever given anyone your home address?

Just because you're not online doesn't mean your information isn't in a thousand digital databases around the country, or world. Because it is. But so is the information of a billion other people. What gets the attention of authorities is the kind of system you're in and what you do to trigger an alert.

Of course the single best way to stay under the radar is to never get in the system. That means, don't attend rallies or protests. Don't get arrested. Don't speed. Don't beat your wife or girlfriend. Don't get drunk and do stupid things.

In short, don't get arrested for any reason, whether you're convicted or not. Your arrest record follows you for life. It affects the kind of jobs you can get (and keep), where you live, your credit report, your insurance costs and so much more. Felonies keep you from voting or holding a license of any kind, even that of hairdresser, barber, and police officer.

A criminal record can keep you out of the military or prevent you from attending certain kinds of schools. It's just not worth it. White collar crime counts too. Embezzlement, shoplifting and bouncing bad checks can be impulse crimes that put you on the government radar for life, even if you're a juvenile.

Parents, if you have kids don't think that you can have their records sealed or expunged. Once upon a time—maybe.

In "the good old days," when law enforcement expunged or erased your record, particularly your juvenile records, they tore a page out of a book, shredded a paper file and your so-called record was gone. In a digital age the term "expunge" is just a fancy word that means the file still exists, it's just inactive until there's some reason for someone to open it again, like to see if you might possibly be a terrorist, patriot, or mental health risk.

After all, if you got naked and streaked in college on a dare from your fraternity brothers and were arrested for indecent exposure, you might do something crazy on a dare in your 40s, like blow something up. That's how the system works—assume the worst and one day you may be right. That's why the six-year old who is suspended for bringing a plastic knife to school to spread peanut butter on his crackers may find himself on a no-fly list in his 20s. Don't laugh. It's not being paranoid, it's being real. A male honor student and athlete whose sister ate waffles in his car and left the knife in the glove box was suspended for 10 days for having a weapon in the car. School officials claimed he violated school policy by having the knife and a penknife he used as a tool for adjusting his car stereo, in the vehicle.

Or, what about the 7-year-old boy who ate his Pop-tart, but the resulting L shape looked like a gun to one of his teachers, so the boy was suspended for shaping the breakfast pastry into a gun shape and waving it around.

The IRS was recently exposed for targeting conservative taxpayers simply for their political affiliation. It had nothing to do with people's digital records.

The real threat to your privacy is not from the government. It's from corporations, businesses and organizations that see your presence, activism or efforts as a threat to their violation of environmental laws, ethical or unethical practices and how they conduct business. There's no logic, reason or reasonable person behind the laws and arrests being made today. When you can arrest and suspend a child for waving a pastry in class, sanity has left the building. Do you want to risk your life and livlihood with a system that responds to breakfast food as a terroristic threat?

The sad fact about privacy is that unless someone wants to steal from you, or steal your identity; or they want to neutralize you because of religious, political or other beliefs, or they want to hurt or destroy you for some personal or professional vendetta you're pretty safe.

Yes, data bases may hold your information and your privacy is at risk, but the chances of anyone using it are slim. So ask yourself, what's most important to you? Being private, safe and under the radar, or speaking out, enjoying your freedom and the rights you have according to law?

It's a choice only you can make.

Technology for snooping, spying, eavesdropping and stalking people used to cost thousands of dollars. It put the art of stealing someone's identity or information in the professional realm because no one could afford to be a professional thief! Now there are so many free or low cost tech solutions that anyone with a few hours to spend online can easily acquire all they need to steal your identity and your financial information. But not every thief is high tech. Many rely on the old standby—stupidity and lack of common sense. For instance:

Are you packing for a trip? Don't load your car in broad daylight, or all at once. Criminals or even neighbors passing by may see you making preparations to leave and mention it in other circles or to other friends who may find it very interesting you'll be gone on vacation.

Don't stop your mail or newspaper delivery. The FBI and US Postal Inspectors say many criminals are working for both newspapers and the postal service. Getting a "hold mail" card be a green light to steal. Better to ask a trusted friend or family member to stop by and collect the mail and newspapers for you. Their car in the driveway and their presence in your home or apartment sents a strong signal that there is someone there, and will often deter a criminal.

If you're out of town and staying in a hotel, be discreet. Don't tell strangers where you're from, how long you're staying and never tell them your room number. They may wait for you to leave so they can enter your room at their leisure and ransack it. Don't talk about your business or what you're doing when you're in a hotel. Be wary of people who are too friendly and too curious about your business.

If you're traveling in an RV or other vehicle, make all your stops for gas, groceries, dinner and the bathroom at least an hour before you plan to pull off of the road. Many individuals or families are first spotted or targeted in stores because of out-of-state plates and are then followed back to their hotel or campground.

When renting a car to go out of state ask for a car with license plates from the state you're visiting if possible. Since most rental agencies have removed their rental stickers to avoid having you stand out as a tourist in a new area, robberies are down. However, a license plate from out-of-state is still a give-away that you're "not from there," and makes you more of a target for criminals.

Part of the fun of being on vacation is meeting new people. Don't be paranoid, but don't be too specific about your plans, your trip and other details. Many criminals frequent tourist destinations for the sole purpose of meeting and taking advantage of friendly travelers. Never give your room number to people.

Meet people at a restaurant instead of your hotel when possible and always let someone know where you are when you go out with someone you've met at a conference or vacation. It wouldn't hurt to snap a photo of them and email it to a friend with details of your plans in case something does go wrong.

When going on vacation or business, don't leave anything in your room, luggage or car that could be used to identify where you're from. If you use luggage tags, put your work address on the tags, not your home. Better yet, use a PO Box or a delivery address such as a concierge at a hotel in your hometown, or a business that accepts packages for travelers. When at all possible do not connect your identity to your address or work and ask neighbors and friends not to give out any information about you to anyone, no matter what kind of story they tell.

If you join any groups or organizations, use your first initial and last name, or just a nickname and last name initial, especially if signup lists are posted on a bulletin board or passed around the room. If organizers insist on your full name, give it to them after the list has already been passed around the room. Request that your last name not be used, explain it's a privacy issue and that while you're happy to give it to them, you'd prefer it not be listed on any public lists. If asked to provide an email address, give an anonymous one, or say you don't use email. You don't have to give contact information, but many groups will request it. If you don't make a big deal of it and just remain silent and never fill out the form, most groups won't notice. Beg off giving phone numbers etc. by saying you have home conditions where such invasions of your privacy would pose a problem. Most people don't push and accept your declining to give up personal information. Simply stating it's a privacy issues is acceptable, although it sends a loud message you're different. Better to just say you'd rather not participate by joining a list.

PRETEXTING

Believe it or not, protecting your privacy can mean being rude, or acting suspicious or paranoid. Don't worry. Better to be thought odd than to have your identity stolen or your home robbed.

One of the most common and successful practices of both criminals and law enforcement is, practice called "Pretexting." It simply means they make up a story to tell you, or someone close to you, in order to get information they can use to steal your identity, determine your schedule or plans, to find out something about you, or to get an advantage over you in some way.

For instance, a Private Investigator may be trying to find out where you work so he can show up to serve a warrant, photograph you, or find out who you are associating with. He will make up a story to tell your neighbor, the postman, or anyone who might know where you work to tell him where you work. He may dress up as a delivery person, knock on your door—knowing you're not home. He'll then go to the neighbor with his pretext that, "This is an urgent delivery for John Doe. He's not home and I have to have his signature to leave the box, only his signature will do. I can take it to his office. Do you know where he works?"

Burglars may show up one day and attempt to deliver something like flowers or a package and knock on a door to find out if someone is home. If there is no answer they'll go to the neighbors and say, "I need to deliver these flowers, or this package. Do you know when your neighbor will be home?"

If you say, "Oh they work late and won't be home till after 7," then you've just told the burglar what they wanted to know—the home owner's schedule. If you want to be a good neighbor you'll say, "I'll sign for it," or better yet, "You know, they keep very odd hours.

They're in and out all day long and don't really have a schedule. There's almost always someone home all day." If you're not comfortable lying, then say, "I don't know." What the criminal is looking for is information about how secure a home is and how noisy the neighbors are.

Another thing to be aware of is that criminals may pretend to be making a delivery to get you to open your door so they can then push their way in. If you must sign for a package step outside the door and close it behind you. If you're not expecting a package ask the delivery person to just leave it, or to leave an authorization slip for you to sign. Those can be slipped under the door, or adhered to the door.

A legitimate delivery person has those forms and is happy to comply and get on their way. Anyone who argues with you about that is probably not legitimate. Call their company if in doubt. Never open the door to anyone you don't feel comfortable about.

Pretext can be something simple, or complex. The person can pretend to be a co-worker, friend, college buddy, or someone related to you or a family member. They then tell a story about needing to find you, contact you or see you—hoping someone will give them a phone number, address or piece of information they can use.

They may use the information to apply for a new credit card. They may use it to find out your schedule so they can break into your home or apartment. What they're using the pretext for doesn't matter. What matters is that you (1) tell trusted neighbors and friends to never give out any information about you, no matter what the story, without contacting you first. Or, (2) don't tell your neighbors anything about your life you don't want known—including what you do, where you work or what your schedule is.

Pretexting works because it's built on a kernel of truth. That's what gets your attention, then distracts you. If in doubt, call your friend or family member to verify they know this person or the person's story. Call from behind a locked door, or from a safe and secure place.

Do not trust strangers, no matter how wholesome, good looking or friendly they are. Do not believe they are long lost friends, school chums or neighors, or that they formerly lived in your home and just want to take a stroll down memory lane. Most serial killers are incredibly charismatic and friendly—that's how they calm their victims and get them to comply. Dare to be offensive. True friends will understand and be glad you're checking out their story. Don't let anyone intimidate you into complying and going along with their story. Chances are they're up to something if they're unwilling to allow you to feel safe by acting cautiously.

SHREDDING

Shredders, the good kind, the crosscut kind, are worth their weight in gold. Buy the best cross cut shredder you can afford and get in the habit of shredding every piece of paper that comes into your hands—from junk mail, medical records, grocery lists to bills, to letters, memos, posters, receipts and even flyers. If its paper it gets shredded. The idea of shredding everything goes back to creating a habit so that when important papers do need to be trashed you're already shredding everything and so they naturally get shredded too.

Once you set your trash on the curb on at the street it becomes public property. Anyone can go through it, including law enforcement, dumpster or trash divers, criminals, nosy neighbors and anyone curious about your life. Shredding, cross shredding especially, ensures that the magazines you read, the offers you turn down, the things you order, buy, rent or sell remains your business, not the business of anyone going through your trash.

Ideally you'd want to shred, then compost the paper, but if you aren't set up for that, at least ensure that all a curious trash picker gets is bags of confetti. Protecting your privacy means ensuring that even your trash doesn't give away any secrets about you!

BUMPER STICKERS AND LICENSE PLATES

Nothing tells people more about you than the car you drive and the bumper stickers you put on your vehicle. Police are trained to profile drivers by the kind and number of bumper stickers on their car. In fact, having an American flag can get you put on a "terrorist" list in some parts of the country.

You can't do much about the make and model of vehicle you own, but you can eliminate unnecessary attention by eliminating all bumper stickers from your vehicle. You can still be passionate about your causes, just don't advertise them on your vehicle. Not only will it get you noticed, but it'll get you labeled and pigeon-holed by those watching you.

The same goes with political signs. If you truly want to keep your views private, don't put up a sign for any candidate, cause or event that could be considered the least bit controversial, unless you don't mind being on people's radar.

People tend to ignore those they see as not having an opinion, cause or organization they identify with. Once people start seeing what and who you support they start forming an opinion, lumping you with a cause (whether you support it or not, they'll assume things based on what they do see you support).

Remember, if your goal is to protect your privacy you have to give up your right to your opinions to anyone driving by. You can still have and support your causes, but be discreet

about when and where. Don't wear it on your t-shirts, post it on bumper stickers, hats or in your yard.

Privacy means just that—keeping your views, opinions and lifestyle to yourself. If you want the government, or your neighbors, to know where you might hang out, go to church, shop or vacation by all means slap a bumper sticker on your car. If you don't, then keep the car clean. Even remove the dealer decal.

Some license plates identify the county and state where you live by the first letters or numbers of your plate. Others put the county beneath the numbers, clearly spelled out. So if you want to keep that information private too, get a "vanity" plate with random number and letters that are hard to remember. The more random the better so that if you are followed it won't be because you have an easy to remember word on your license plate.

When it comes to privacy and vehicles, keep your car clean inside and out. Fast food bags, shopping bags, personal items and equipment are a give-away for where you shop, hang out, eat and frequent. If you go to a gym or other class, put your equipment in your trunk, not the back seat. If you don't like putting things in the trunk, then use an empty box, or a towel or blanket to cover items in the seat. I

If you go shopping and then put items in the trunk and plan to go back inside, move your car to the other side of the shopping center. Crooks or opportunists that see you put packages into the trunk then leave know they can easily pop your trunk and be rewarded because you're still shopping.

The hassle of driving to the other side of the mall is much less hassle than having everything you just bought stolen, and then having to have your trunk lock or trunk repaired. Take the time to move the vehicle.

DROPPING OFF THE GRID

It's a popular dream—dropping off the grid and "disappearing" from all official records, functions, lists and databases. It's a very difficult one to achieve. It's not impossible, it's just expensive. The fact is, anyone can disappear and not be found, unless there's a significant amount of money involved.

Disappearing is easy as long as it's not in someone's financial interest to find you. A Private Eye who is being paid $100 an hour to find you has far more incentive to dig than the magazine company you owe $12 to. The farther off the grid you go, the more it costs to find you.

The only people who will bother looking for you are the ones who believe you have or are something of

value to them. The more private you are, the harder you are to find and the more it will cost someone to find you. The more walls and diversions you create in the name of protecting your privacy, the less likely people are to try to invade your privacy, or be able to find you.

There are dozens of great books on how to disappear, but the best way to disappear is to protect your privacy. Not only does it become impossible for people to steal your identity, it becomes practically impossible to find you.

Are you ready to drop off the grid and protect your privacy by disappearing? Here's a hint. Don't go out and buy a book on how to do that using a debit or credit card, or even search online for such items from your home computer. If you're serious about staying off anyone's radar, then pay cash and go to a bookstore where you can buy the books you're interested in without leaving a paper or digital trail.

- ✓ Wear sunglasses or a wig or a floppy hat so surveillance cameras don't show your clear identity. Don't use your buyer's loyalty card. Leave your debit and credit cards in your RFID wallet.
- ✓ Don't talk about your plan with anyone. Be discreet. Remember, the only way a secret is safe between two people is if one of them is dead, and even that is no guarantee. People's journals and emails survive them.

Things you'll want to do to begin to remove yourself from the radar:

- ✓ Never associate your name with your address. If you rent an apartment or home, get a place where utilities are included so your name doesn't end up in the utilities database.
- ✓ Use a Post Office Box for all correspondence.
- ✓ Use a nickname or initials on your correspondence, and don't spell out your entire name.
- ✓ Create a false persona, including birthdate, (don't use the same year or month of your own birthday either) and school affiliations. When you create accounts use this persona as your character. Use photos of objects (trees, nature, dogs etc that are unrelated to you in any way) for profile photos. Use Skype for a phone number and never give out your cell phone number. Have all calls forwarded to your cell phone instead. These won't prevent people from finding you, but they'll make it more expensive for people—which means they're less likely to pursue you because of the cost of finding you.
- ✓ Use "burner" or one time use cell phones. If you have an iPhone or Android phone you can create a

"burner" phone number by going to: http://burnerapp.com/ , downloading and creating a phone number for an hour, day or week. This is a great application for avoiding sales people, when meeting strangers in a bar or conference, or when you just need a phone number for a short time and then don't want to be bothered again.

Privacy is and has always been a concern for many. It's very hard in today's world to just drop off the grid without moving to another country or starting over. It can be done and is done every day by people who don't want to be found, or who value their privacy. Only you can decide if you want to protect your privacy 100%, or just enough to keep your family, your identity and your finances safe.

- ✓ address, workplace or other information to someone you've never met in person.
- ✓ Educate yourself. Use http://duckduckgo.com to conduct online searches that aren't stored and tracked.
- ✓ Buy and use a good cross-cut shredder.
- ✓ Use common sense when traveling or moving about in public.
- ✓ Protecting your privacy is a full-time job that's up to you to do right. You can't totally disappear

Sit down and ask yourself how much privacy you want and need. Create a plan to protect and harden the security on your digital devices. Educate yourself about encryption and your rights. Sign up with a company like LifeLock or add extra security to your credit reports by visiting or calling the three major credit unions (TransUnion, Equifax and Experian) to find out how to protect your credit.

- ✓ Learn how to turn off the GPS locator service on your laptop, iPhone, smartphone and other digital devices.
- ✓ Don't trust anyone you meet online—and never, ever, ever give your personal information, name,

unless you've got the money and the resources. But realize that if someone wants you found the primary factors for them finding you are (1) What's it going to cost? and (2) Is finding you or the information about you they want worth what it's going to cost them?

- ✓ Subscribe to JJ Luna's website(s): http://www.jjluna.com Luna is a man who's taught millions of people how to disappear, or become invisible. His newsletter offers dozens of tips for those who are serious about disappearing.

101 WAYS TO PROTECT YOUR PRIVACY

There are thousands of things you can do to protect your privacy online and off. Here are 101 things you can do now to ensure your privacy is protected today:

1. **Turn off the GPS locator functions in all your digital devices, including laptops, cellphones and apps.** Make sure your children's GPS locators are off too.

2. **Stop using apps like FourSquare to "check in" and let the world know where you are (barber, coffee shop etc).** Why do you want to alert the world to the fact your home, business or office is empty because you're at a movie?

3. **Understand what an app does before you download and activate it.** If you read the terms of service you'll see that many apps, particularly the free ones, use location sensitive information to funnel ads to your phone or tablet when you're out and about. This may mean turning on the very GPS functions you just disabled!

4. **Never, never, never ever post your home address, phone or identifying information online on any social media website, even the ones that say they won't share them.** Especially don't post personal information on Facebook because they do share it with every "friend" on your list whether you want them to or not.

5. **Only friend people on Facebook, LinkedIn or social media sites that you know personally or have a reason to know (through work etc).** Google them to find out if they are a "real" person (do they have photos of themselves, a blog, a website, are they in a company directory, do they have more than 50 friends or any kind of a web presence **you can verify?).**

6. **If you have children put a keylogger on your computer and use it.** You're not a horrible parent, you're a concerned one. Use any and all parental controls and programs you can to ensure an older, more tech savvy and social engineering pedophile is not targeting your children. Kids like to think they know how to handle themselves and how to spot a predator, but they don't.

7. **If you have children put the family computer in a public room in the house where you can keep an eye on what they're doing online.** Block porn sites and other unsafe sites. If you don't know how—learn, or pay a professional to walk you through it so you learn how.

8. **Do not ever get on the police radar for doing stupid things, like speeding, breaking the law, DUI, domestic disputes,**

neighbor quarrels or protesting. Once you're on the police radar you have a rap sheets and are more likely to be looked at or considered guilty of any crime or offense related to the one you committed. If you hit your wife, get in a shouting match with a neighbor, drive drunk and get pulled over, every time there's a domestic dispute within 10 blocks of you your arrest is going to pop up when a neighbor hits his wife and police are called. Bottom line, don't get arrested.

9. **Don't post threats, or even joke about threats anywhere online.** There are plenty of people doing time for typing, "I'm gonna to kill you. You're such an idiot." Years ago people understood you were angry and posturing and didn't really mean you were going to kill anyone. You were just letting off steam. Today the police take those comments seriously and it doesn't take much for them to arrest and charge you with terroristic threatening.

10. **Conduct your life as though every second was being recorded, because it probably is.** You may not see the CCTV cameras, or the dozen cellphones that are recording your juvenile outburst at the kid at Burger King who screwed up your order, but they're running anyway. Chances are good you'll end up a YouTube star when your outburst goes viral. Control your temper. Do not end up a YouTube sensation for being a jerk.

11. **Think twice about what you post to YouTube or Viemo.** Sure, everyone wants their 15 minutes of fame, but which do you value more, your privacy or your 15 minutes of fame?

12. **Be aware of what your kids, wife and friends are posting.** You may not post any photos of yourself, but are your friends and family a little freer with their posts? Ask people not to tag you or post photos or video of you; or just don't go to events where people are taking pictures and video. If that's not possible, then don't do anything at the event that could be misconstrued if someone else saw it.

13. Don't let others use your computer, laptop or cellphone. Anything anyone does on your devices is going to be attributed to you. Letting your kids surf and play on your cellphone may not be any big deal, until they tweet, post or—like one recent 3-year old did, click around and

buy a car using your ebay account.

14. **Only keep the credit and debit cards you use most in your wallet.**

15. **Buy RFID sleeves to shield your debit, credit and bank cards from crooks with RFID readers or scanners.**

16. **Never carry your social security card in your wallet or purse.**

17. **Ask why someone wants your social security number and decline it. It's not legal to use it for identification (says so on the card itself) and only a handful of agencies have the right to ask for it.**

18. **Check your credit report monthly using any of the credit reporting services available through the three major credit services: TransUnion, Experian or Equifax.**

19. **Do not put bumper stickers on your car or vehicles.**

20. **Do not wear "message" t-shirts or controversial slogans.**

21. **Keep your vehicle clean and fully operational and functional inside and out to deter police and other law enforcement officials from stopping you, "Just because."**

22. **Obey the law.** This should go without saying, but people often don't realize that a police record puts you in the system and being in the system is the first step to having your privacy eroded.

23. **Don't use home office deductions.** When you deduct home office space or any other deductions you give the IRS and the government the right to come into your home or office to examine it to ensure it meets proper guidelines. Same with having a non-profit or getting food stamps or government assistance. When you take money from the government they have a right to examine your home, business, office etc.

24. **Don't get a rescue dog, cat or animal. It seems cruel, but read those adoption papers carefully.** Most rescue organizations make you sign a contract with small print that makes you agree to they have the right to come into your home at any time for any reason, or no reason and examine every inch of it and your life if they "believe" the animal you just adopted, "might" be at risk. Guess what.

They might bring a police officer or other official with them who has the right to walk around your home and property without a warrant as well.

25. **Don't accept government aid, food stamps or other help if you can avoid it.** If you need to accept food from a food bank or register to receive food, realize your name is going into a database that will erode more of your privacy.

26. **Give generously, but give anonymously.** Donors are rare and so when people do give organizations enter their information into a database and sell or circulate it among organizations who will then also target you for your money. Give cash, money orders without your name on them, or give and give anonymously.

27. **Be cooperative and quiet if interviewed by the police for any reason.** Saying nothing, or saying too much both make police alert on you even if you haven't done anything but witness a crime. Think twice about volunteering to be a witness in a crime. You don't know who the perpetrator is and how motivated they may be for you not to testify. Pick and choose your battles carefully. Only you know which matters more—privacy or justice. Choose wisely with your long term goals in mind.

28. **Learn your way around your computer.** Take a class at your local community college, ask a trusted and knowledgeable friend to tutor you, but learn how to erase files, download apps, install software and look for viruses and malware.

29. **Don't store files and information on your computer you don't want anyone having access to.** Chances are no one will ever find it, but it could happen.

30. **If you must store financial information on your computer, encrypt it.** If you don't know how to encrypt it then make it hard for criminals to find. Name it something like "Summer vacation photos," or "December newsletter," and not, "2013 Tax returns" or "My Social Security Number." Make the file name something you'll remember, but that someone searching for bank or credit card information won't easily find.

31. **Create an online persona with fake birthday and other personal information so thieves hacking your Facebook account or other social media accounts won't**

be able to use to hack your banking or other information.

32. **Change your passwords frequently, at least every three months.** Use upper and lower case letters, numbers and symbols. If you have a hard time remembering your passwords, write them in a notebook and store them away from your computer or desk.

33. **Teach your children about Internet safety and review the information with them frequently.** Establish rules about never sharing personal information like last names, addresses and phone numbers with people they meet on the Internet.

34. **Never share dates or details about vacations, trips or expensive purchases online.** This means don't post photos or even talk about your purchase. Don't post photos of your home, car or possessions online. If you got a new gun, television, car or home theatre don't tell the world. Some of the world may find you and visit you one night.

35. **Be aware of your surroundings and notice if people, cars or others follow you home.** When you come out of your home in the morning, or walk to your car at work or at the mall, take a few minutes to look around the parking lot, or on the street to see who is there. Are there people sitting in cars? On benches? Jogging by? Riding a bike, or just hanging out? Be aware they may not be casual bypassers.

36. **Use luggage and ID tags with your work address or a post office box number, or the address of a business that will hold packages and items returned to it.** Check with businesses like FedEx, UPS, Kinkos and even the USPS's "mail forwarding" services. They charge a fee for forwarding lost (or stolen) luggage to you, but it's safer than having a stranger steal your property, claim they "found" it and then try to return it to you at your home or office where they can then case your place for a future robbery or home invasion.

37. **Carry a "throw away" wallet.** Carry an old wallet with $20 and some expired gift cards and fake papers that you can give a thief if you are mugged. Keep your real wallet in a front, inside pocket or travel pouch and your throwaway wallet in your coat or back pocket where you can easily reach it and give it to thief who only wants to rob you and run.

38. **Don't put your name, phone number or address inside of controversial books you might lend out.** Either buy two copies and keep one for your own library and lend the other, or don't lend books at all.

39. **Don't put political signs or banners in your yard or on your property.**

40. **If filing a police report for a crime against you, ask police NOT to put your Social Security Number on the report.** Ask that all personal information be blacked out and then go down to the police station within the week and check the report yourself to see if personal information was indeed listed on the report.

41. **Don't tell friends, neighbors or others that you own a gun or keep guns on your property without just cause or reason.** Only you can decide what that is. It's up to you what you tell your children's friends parent's about your guns, but realize that the very act of sharing that information can compromise your privacy.

42. **Whenever and wherever possible, remove your name from websites that list your name and address.** Keep your name and address separate as much as possible. If you're not sure how to do this go to:

- ✓ MyLife.com
- ✓ Acziom.com
- ✓ Intelius.com
- ✓ ZabaSearch.com
- ✓ Spoke.com
- ✓ BeenVerified.com
- ✓ PeekYou.com
- ✓ USSearch.com
- ✓ PeopleFinders.com
- ✓ PeopleLookup.com
- ✓ PeopleSmart.com
- ✓ PrivateEye.com
- ✓ WhitePages.com
- ✓ USA-People-Search.com
- ✓ Spokeo.com
- ✓ PublicRecordsNow.com
- ✓ DOBSearch.com
- ✓ Radaris.com

Search the site FIRST to make sure you're listed. They usually have your legal name, aliases, age, current and previous addresses, and family members, but anyone can pay to see more

(like your criminal record, bankruptcies, and more).

Second, email Support@BeenVerified.com with the following template filled out with your info:

```
Dear Been Verified
Customer Support:

As per your privacy
policy, please remove my
listing from your
databases:

a. First name:

b. Last name:

c. Middle initial:

d. Aliases & AKA's:

e. Current address:

f. Age:

g. DOB:

Thank you for your
assistance.
```

43. **Third,** you'll get one email saying they received your opt-out request, and another confirming you've been deleted.

44. **Learn to use anonymous email addresses, like hushmail.com.** There are a variety of websites that offer anonymous email accounts, hushmail.com is just one. For even more privacy and security you'll need to disguise your login as well. Setting up a pseudonymous -webmail account is "a prudent first step", according to the EFF. But it's easy to trace the IP address used to log in to that account, then see what other accounts have been accessed from the same address.

45. According to WIRED Magazine it's best to use Tor, a system that masks your IP address: go to torproject.org to download the browser bundle. Always use it to log in; one login with your real IP address will be permanently traceable. "Do not give your -webmail provider any information linked to your real-world identity."

46. **Subscribe to websites like: http://lifehacker.com, WIRED.com, kommando.com and others** (using your anonymous email address of course) to learn about how to protect yourself and your privacy).

47. **Never use anything in your emails or email signatures that gives your name, address, work info, personal info or anything else that could give away your identity.** Even though anonymous websites are anonymous to the public, law enforcement can look at emails all they want and Hushmail and

others must comply with those orders. Not having any identifying info in your account can protect your privacy. You might even want to change accounts frequently. Use a Google Voice or Skype number, not your real cell or home phone number. Use those numbers to forward calls to your cell phone.

48. **Learn not to be a creature of habit.** When you go to work or school the same time, the same way every day you give up some privacy to anyone wanting to figure out your routine. Change it up. Go a different way, or 30 minutes earlier. Leave in time to go have breakfast someplace before work, or dinner after work. When you become a creature of habit or routine you give up some privacy.

49. **Don't write your name on your stuff**. Summer camp should be the only time you put your name on anything you own. When you sew, write or tuck a business card into your clothing or property you guarantee whoever finds it can find you, but do you want that?

50. Use services like mail forwarding services that have a permanent address, but that wait for you to notify them of where to send your mail. They are discreet and will not give out your address except to law enforcement agencies who have a warrant. They are mostly used by RVers who have numerous address changes during a year. They can send your mail or items to a different address every day if you want. They charge a set fee and postage.

51. The most popular mail forwarding service used by RVers is Escapees.com. There are other sites for sailors and people who move around the world via water, cruise ships etc.

52. **Use common sense.** Be careful who you friend or befriend online or in real life. Take time to get to know people before inviting them to your home.

53. **Put away photos, keepsakes or items that offer visitors an inside look into your life before inviting them over.** This is extreme, but not so much. Limit areas of your home to public view if you want to protect your privacy. If you have block parties, meetings, open houses or parties, it's okay to lock doors, put away items that feel or are sensitive to you, and to limit access to information about you to visitors.

54. **Just say no**. Learn to set and enforce boundaries. People are nosy. Even innocent, but nosy

neighbors may want to go through your medicine cabinet or drawers or files if given the chance. It's okay to say "No," to people who ask invasive or personal questions about you, your work or your life. You can respond: "That's an interesting question. Why would you want to know that?" and put the ball back in their court, or you can simply say, "I don't talk about my work, company policy. But what do you do?"

55. **Don't give contractors the run of your home.** Many, many contractors have jail or prison records, addictions and other issues that make them security risks. That's not to say all plumbers, vendors and contractors are potential thieves, rapists and burglars, but why take the risks?

56. Put away knick-knacks, lock up prescription drugs and take all medication other than aspirin out of your bathroom cabinets and closets. Limit traffic to certain areas of the home, lock inner doors and have someone in the home when the work is being done. Don't just give out keys to contractors. Lock your filing cabinets.

57. Use licensed and bonded businesses and insist on the names (and even photos) of all members of work crews that have access to your home. Blame your seeming "paranoia" on a story you heard about, read about or know from a neighbor. Don't worry about offending anyone. It's your privacy. You can do these things discreetly and matter-of-factly. Honest contractors understand.

58. **Learn the laws of your state.** Some states can take your DNA against your consent, while others can only fingerprint you and get your DNA if you're suspected of a crime—another reason not to cross paths with the law.

59. **Get rid of your loyalty cards, or create new ones under a different name.** Getting 5 or 10 cents off a product at the grocery store on items you buy is great. But grocers and other businesses are building a profile on you that they sell to other businesses, including insurance agencies. If you buy tobacco products, diet and weight loss products, products for incontinence or other over the counter supplements etc. that tells a lot of people that you may have issues with your health; information that can find its way to life and health insurance companies who can then deny or raise rates for services. If you

don't believe you're being profiled, ask yourself why, if you buy dog food for instance, you're offered coupons for competing dog food when you shop.

60. **Monitor your credit and debit card use.** Everyone else is. When you start buying groceries or other items on a credit card you only used to use for car rentals and business trips, credit card agencies will often reduce your credit line, thinking that you've lost a job or can't afford to pay for the basics (like food and rent) and are about to charge up your card and default on payments. So they reduce your credit line. Still think your purchases are private? They're not.

61. **Pay cash while you still can**. All your purchases, down to the color, size and number, are permanently recorded every time you make a purchase with a debit or credit card. We're moving towards a cashless society quickly, but we're not there yet. Keep your purchases private by paying cash as much as possible. It's not that any one item is bad, but a pattern or history of buying certain things can create a profile of you that violates your privacy. Larger stores, like Walmart, embed certain products with RFID chips (shaving razors and food for instance) that start being tracked the minute they leave the shelf. Once you buy them with a credit card or debit card, that purchase is also tied to you.

62. **Don't use public WiFi to check your email or other accounts.** Anyone, anywhere around you can easily see what your passwords are, or what your bank balance is. Limit your internet use in public places, including hotel rooms.

63. **Don't conduct personal business on company computers — especially laptops.** You may work for the best company in the world, but chances are they've got keyloggers and other software on that laptop they've loaned you, and certainly on the desktop you use, so they can monitor how you use it. Avoid the temptation to use a company device for anything personal.

64. **Don't tag your photos and ask friends not to tag theirs.** Once that photo of you is on the Internet there's no getting it back. Even if you use a nickname, there are people who can link the nickname to you.

65. **Don't give your address or other information to meet-up groups or other online communities who like to socialize offline.** Use a mail-forwarding company, PO Box or just decline to give up the address in the name of "safety" until you feel comfortable. This is easier for women to do rather than men. Men who are cautious about their safety may be perceived as having criminal intent rather than just being cautious.

66. **Don't brag**. The minute you start bragging about possessions, raises, accomplishments and things you've acquired you attract attention, and not all of it is the kind of attention you want. Be humble. Limit sharing your good news with trusted family and friends.

67. **Don't give your hotel room number.** Don't give out your business agenda, room number or other information to anyone you don't know personally, and don't share schedule information (when you're out or in or where you're going) with anyone, especially with casual connections you may make in the hotel over breakfast, dinner or while in the lobby.

68. In areas known for their convention traffic criminals will often strike up a conversation with hotel guests under the pretense of being a fellow attendee. They'll find out what conference you're attending and use that time frame to break into your room, or to pretend to be you to talk the maid or housekeeping crew that you (they) forgot their key.

69. Don't let anyone connect you, your room and your schedule. If someone wants more information, ask them for a card or their information and tell them you'll contact them once you're back in your office.

70. **Use code letters or names for sensitive information.** You're not being paranoid. You're doing what medical offices, the military and hospitals do to protect patient records. Next time you're in your doctor's office notice how your personal file is set up. There are colored tabs to tell the staff your age, medical status, condition and even what insurance carrier you use.

71. It's convenient, but it also keeps those who don't know the code from reading your charts. Medical studies will refer to you by number, not name. If you have a file you want to keep

private, consider labeling it something unrelated. It may not prevent its theft, but someone who has to go through 300 files looking for the "Jones" account which is really labeled, "Michigan vendors" because Jones is a Michigan vendor, or grew up in Michigan, and you'll at least slow them down.

72. **Lock up sensitive items.** Yes, it's a pain to go to your bank deposit box, or to a safe in the basement, but locking up your sensitive items (passport, social security card, spare cash etc) will keep them safe. Be careful about safe deposit boxes as some people are reporting items disappearing out of their safe deposit boxes. Better to install a safe in your home (encase it in concrete in a floor or secure it to a floor or wall) that will hold items you want to protect.

73. **Limit the number of credit cards you have and use.** Many people like owning 10 or more cards, but the more cards you have, the more your identity is at risk. Own two to four cards and make sure you check purchases and limits on them monthly.

74. **Use apps like PROTECT MY PRIVACY and DISCONNECT2.** Apps like http://www.protectmyprivacy.org/ and Disconnect 2, provide more protection and privacy for your iPhone and computers. Disconnect 2 stops over 2,000 third-party sites from tracking the personal information you input online.

75. Once downloaded, a toolbar on the browser gives a real-time view of the websites that would be grabbing information about your search habits or recent location check-ins were you not using the tool. Not only does it block the transmission of browsing history, Disconnect encrypts data you choose to share on sites, just in case it one day falls into the hands of a separate company or person.

76. **If you think you've been phished, scammed or hacked, report it.** Even if you're not sure you've been spammed, don't take chances. If you suspect you've received spam or phishing emails (that are trying to scam you for private information like log-ins and passwords), then forward them directly to the FTC's database for spam with the full header information, or send to the Anti-Phishing Working Group. The FTC's email is: spam@uce.gov and the Anti-Phishing Group is: reportphishing@antiphishing.org.

77. **Remove yourself from LinkedIn's ads.** Facebook has already done this, much to the vocal objection of Facebook fans. LinkedIn recently followed suit, making changes to its privacy policy to automatically include your name and photo in its social ads by default. You can still opt out of their ad program though. Go to your LinkedIn Settings account at the top right hand side of the page after you sign in. Click on "Settings," then click on the "Account" section (towards the bottom left), then "Manage Social Advertising" link. Uncheck the "LinkedIn may use my name, photo in social advertising" box and click save. That will opt-out your choice.

78. **Use your hotel room safe for paper and files as well as other valuables.** Don't leave information, mail or other items that can identify you, in your hotel room. It may be a hassle, but keeping your briefcase in the trunk of your car, or papers in a hotel safe can help protect you from someone stealing your identity.

79. **Think before answering.** Some of the best social engineering criminals make the best conversationalists. They know how to get people talking and giving up information they don't even realize they're sharing. How? People like to talk about themselves, their work, their hobbies and their accomplishments. When talking to strangers or people you've just met at a conference, keep the conversation about them, not you. If they ask a personal question about your dog's name, or your kid's names, ask yourself why. Pet names, kid's names etc. tend to be words people use for security questions or passwords. Strangers really don't care about the names of your kids and animals. Why would they? Decline to answer, or make something up. The US Navy Seals do. Most of them that are online use a totally bogus name, history and even location so they can keep in touch with real friends without giving away any personal information.

80. **Check your computer frequently for viruses.** It wouldn't hurt to wipe your hard drive and operating system frequently if you have a lot of files or information you must keep private.

81. **Get a Post Office Box and use it.** Send mail to yourself, then to a nickname with your last name, then to a completely benign and foreign name.

82. **Use external drives to store your files**. You don't have to store files on your computer. You can save them to external hard drives or thumb drives then lock them in a safe or hide them in your home or office.

83. **Do not use FREE software, FREE Templates (Wordpress) or FREE anything downloaded from the Internet.** Chances are it's malware or adware, or worse. Pay the $10, $20 or $100 for the real version.

84. **Do not watch porn.** Porn sites are virus factories for malware, adware and phishers, scammers and hackers. If you're watching porn, particularly free porn, you're 99% likely to have a compromised computer. If you've been watching porn, erase your hard drive completely and reinstall your operating system.

85. **Don't sign up for marketing lists.** Usually disguised as surveys, polls, sweepstakes and contests, these things are really marketing lists designed to help profile you and to sell you more stuff. If you really want to win something, buy a lottery ticket. Your odds are better and you don't have to give anyone your name or address until you actually win something.

86. **When paying for a purchase and a clerk asks for your zip code, politely decline.** They don't need it to complete your purchase and will most likely use it to empty your bank account since it's a security backup to your card number.

87. **Your vet, hardware store and most other folks you interact with have no legal or legitimate need to know who your employer is or what your SSN or phone number is.** They're asking because they're building a database. You are free to give them a bogus or fake number. We are socialized to be polite and give up any information someone asks us for, but fight that urge. Just say no.

88. **Do not open your door to any delivery man or person you do not personally know.** What has this got to do with privacy? Because the "delivery scam" is the oldest one in the books. Anyone can get a delivery uniform and pose as a delivery man to force their way into your home, steal your purse, rob or rape you.

89. **Remember that anyone can be found, any secret discovered and any encryption cracked.** All it takes is enough money. Instead of trying to be 100%

invisible, make it very, very, very expensive for anyone to find you, your files or your secret. Most people will not spend the money or invest the resources to crack your life open unless it is worth it to them for some reason.

90. Parents may spend a fortune to get their child back from an ex-spouse, but not unless they have those funds. Most people will not spend a fortune to get a trivial piece of information. People rarely spend $100,000 to recover $10,000 in loans. Make it expensive for people to find out things about you and most will move on in search of a different target.

91. **Never give out your home address, correct date-of-birth or to anyone other than a government agency.** There's no legal reason for them to have it. A post office box will do just fine. No matter what that guy in the blue shirt at Best Buy says, he does NOT need your SSN to sell you anything.

92. **Pay Cash Whenever You Can.** Get in the habit of paying for all purchases with cash. When you pay cash for items, from food to gas, you eliminate the paper trail, don't have to show anyone your driver's license or other ID, and you don't let anyone know where you're from, or give any indication you're from out of state (other than an accent), or out of the area, a tourist etc. Use small bills and don't flash a wad of cash.

93. **Put a Google alert on your name.** It's free, but you must have a Google account (also free) to do this. That way anytime anything about you that includes your name (photos, stories, blogs etc) pops up on the Internet, you get an alert and a link to the content and deal with it as you see fit.

94. **Put passwords on ALL your digital devices, not just your computer.** Yes, it's a bit of an annoyance to have to enter a password every time you want to access your iPad, tablet, cell phone or laptop, but the privacy something as simple as a password gives you is priceless.

95. **Sign-out of EVERY site you use or visit when you're done**. This includes Facebook and all social media sites. Not only does it prevent someone else from sitting down at your computer and not having to sign in, it keeps your content private.

96. **Protect your phone calling information.** The government is after your information, while at the same time protecting it.

According to the FCC (Federal Communication Commission) "Providers of telephone service, which include local, long distance, and wireless phone companies, as well as Voice over Internet Protocol (VoIP) service providers, collect customer information, such as the numbers you call and when you call them, as well as the particular services you use, such as call forwarding or voice mail. This information is often referred to as Customer Proprietary Network Information (CPNI). Telephone companies may use, disclose, or permit access to your customer information only in the following circumstances: 1) as required by law; 2) with your approval; or 3) in providing the service from which the customer information was obtained.

97. Your telephone company may only release your customer information to you upon request with certain protections, such as a password if your request is by phone or online, or with valid photo identification if your request is in person.

98. Your telephone company must notify you immediately when it creates or changes a password, a back-up for a forgotten password, an online account, or an address of record. Your telephone company may use your customer information, without your approval, to market enhancements to services you already use. If your telephone company uses your customer information for other marketing, it must obtain your approval to do so.

99. Your company must keep accurate records regarding disclosure of your customer information to third parties and your approvals. Telephone companies must submit to the FCC an annual certification attesting that they are abiding by these rules, and a summary of all consumer complaints received regarding unauthorized release of customer information.

100. To find out more about FCC rules protecting your customer information, see the FCC's consumer guide."

101. **Turn on 2-step verification if you have a Google account.** Yes, it's annoying to enter a password, then have to get a verification code to sign into your email account, but it keeps criminals from getting access to your email even if they hack your password. This simple little step turns your phone into a security fob. Meaning, in order for anyone to get into your

Gmail account from a new device, or even your desktop, a person (hopefully you) needs a code that's sent to your phone.

102. It's helpful if you don't want parents, partners or kids, or co-workers hacking your computer while you're traveling. Just make sure you have your phone, or a printable page of codes, with you when you travel. If your phone battery dies, the codes are a great backup, and you can only use each one once.

103. **If you use Facebook, make sure your settings are set to private, not public.** Otherwise anyone on the Internet can see what you share, say, post. You shouldn't be posting all that stuff anyway, but chances are you have or are. And, once people know who's on your friend's list, they become weak links apt to share their knowledge with strangers too.

104. **You may be anonymous, but your IP number probably isn't.** Use an IP masker like http://hidemyass.com or https://www.torproject.org/ to mask your IP addresss so spammers and hackers can't see or find you. These sites and applications aren't a 100% solution, but they do amazing things to protect your surfing if you read and follow the advice and protocol outlined on the site.

105. **Learn to change your habits.** The easiest way to find out about a person is by observing their habits and routines. We are creatures of habit and hate to change our routines. If you're serious about protecting your privacy you'll have to take steps and change patterns you've grown comfortable with. Vary your routines. Go to new restaurants. Don't take the same route home from work or to work.

106. **Get in the habit of clearing your browser history and cache on your computer.** It doesn't matter if you're the only one using the computer, or if you live alone. Anyone with access (breaking in etc) can access your surfing history by gaining access (physical or remote) to your computer.

107. **Turn on your firewall and leave it on.** If you aren't sure what a firewall is, or how to turn it on, contact your Internet Provider's tech department and have them walk you through the process. Or, go to http://duckduckgo.com and search for a tutorial online.

108. **Only provide the purchase date**, model/serial numbers, and

your contact information of warranty registration forms. Companies don't need any other information.

109. **Never ever, ever give out ANY personal information, nor confirm or deny any information from a caller to your home.** If you didn't call a known number to conduct a transaction, then don't answer any questions from anyone calling your number.

110. **Never answer telephone polls about any topic, whether it's business, political or other.**

111. **Keep a list of your credit cards and other sensitive financial information in a secure place, but black out your name on the card.** That way even if the list is somehow stolen or compromised the thief won't have your name or the name on the card along with your card number, making it much harder to use or sell the information.

112. **Add your name and phone number to the "Do Not Call Registry."** Tell companies you do business with to remove your name from customer lists they rent or sell to others.

113. Utilize the services provided by the Direct Marketing Association to remove you from most national telemarketing, mail and e-mail lists.

114. The federal government's Do Not Call (DNC) Registry allows you to permanently restrict telemarketing calls by registering your phone number at donotcall.gov or by calling 1-888-382-1222. If you receive telemarketing calls after your number has been in the national registry for three months, you can file a complaint using the same web page and toll-free number.

115. Call the credit reporting agencies' notification system at 1-888-567-8688. This will reduce the number of unsolicited credit and insurance offers you get. All three major credit bureaus participate in this program. You also may submit your request to opt out online.

116. Under U.S. Postal Service Rules, it is illegal to send mail that looks like it is from a government agency when it isn't. It is also illegal to send mail that looks like a bill when nothing was ordered, unless it clearly states it is not a bill. Report violations of this rule to the USPS.

117. **Protect yourself from Medical Identity Theft:** Personal information you give to your

doctor is shared with insurance companies, pharmacies, researchers, and employers based on specific regulations. The privacy of your health records is protected by federal law (the Health Insurance Portability and Accountability Act, also known as HIPAA), which:

118. Defines your rights over your health information

119. Sets rules and limits on who is allowed to receive and/or see your health information

120. The U.S. Department of Health and Human Services Office for Civil Rights (OCR) (1-800-368-1019) is an excellent resource for complete details and advice about the HIPPA ruling. Along with fact sheets and educational materials, the OCR also provides a listing of resources for consumers, providers and advocates. According to the US Government:

121. Like traditional identity theft, medical ID theft can affect your finances, but it also can take a toll on your health. Some ways you might detect medical ID theft include:

122. You get a bill for medical services you did not receive.

123. A debt collector contacts you about a medical debt you don't owe.

124. You find medical collection notices on you don't recognize on your credit report.

125. Your health plan says you've reached your limit on benefits when you know you haven't.

126. You are denied insurance because your medical records show a condition you don't have.

127. If you believe that a person, agency, or organization covered under the HIPAA Privacy Rule violated your health information privacy rights or committed another violation of the Privacy Rule, you may be able to file a written complaint with the Department of Health and Human Services, Office for Civil Rights.

128. **Buy paperback books, not digital books.** Amazon.com and other ebook readers collect more information on customers than any other source. Not only can Amazon tell what books you bought, how you paid for them, or how often you read them, they can also tell how long you spent on each page!

The Reader Privacy Act prevents them from using this information for marketing purposes, but they still collect and store it in case law enforcement officials want it. The Digital Due Process Coalition is helping fight this collection of information and is an excellent source of additional information: http://www.digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163

129. **Pay the extra $10 or so a year to get privacy protection for your URL or Domain Name if you have one.** Go to http://privacyprotect.org/contact/ or http://whois.com or your Internet Provider for more information.

130. **Close your curtains, lock your doors (car and house) and secure your windows and property with good locks and consistent diligence.** Check your locks every night before going to bed. It's simple, but effective. Criminals can case or explore your house from the comfort of their vehicle with high-powered binoculars and other surveillance devices.

They can see where you put items, where safes, valuables and other high-dollar items are kept. They can get a very good sense of your worth by seeing the inside of your home. If you like the sun shining in, then consider moving expensive items like flat screen televisions and stereo equipment to rooms inside the house. Take time to go out on the street and see what you can see through your own open windows.

131. **Think like a criminal and then act to protect your items.** The way police officers and others who investigate crimes are trained is by teaching them to think like the people they are supposed to catch. They actually try to figure out how they would steal something so they have an idea of how a thief might steal it too. They try to figure out how to commit the perfect crime so they can prevent it.

Do the same. If you were a criminal, a phisher, a thief, how would you gain access to your information, finances and privacy? Once you understand that, you'll know better how to protect yourself and your family.

FOOTNOTES

1. Hacker's Demo Shows How Easily Credit Cards Can Be Read Through Clothes And Wallets http://www.forbes.com/sites/andygreenberg/2012/01/30/hackers-demo-shows-how-easily-credit-cards-can-be-read-through-clothes-and-wallets/

2. Federal Education and Privacy Act (FERPA) http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

For additional information, you may call 1-800-USA-LEARN (1-800-872-5327) (voice). Individuals who use TDD may use the Federal Relay Service. Or you may contact Officials about FERPA at the following address: *Family Policy Compliance Office U.S. Department of Education 400 Maryland Avenue, SW Washington, D.C. 20202-8520*

3. TECHNOLOGY: ON THE NET; The F.B.I. sting operation on child pornography raises questions about encryption.

http://www.nytimes.com/1995/09/25/business/technology-net-fbi-sting-operation-child-pornography-raises-questions-about.html

4. Encryption is evidence of illegal activity http://blog.emagined.com/2009/09/09/encryption-is-evidence-of-illegal-activity/

5. Jordan Maxell 3-Maritime Law Rules the World Commerce and Courts www.youtube.com/watch?v=AxDfBpcjKgs

6. West Virginia Boy Arrested Over NRA T-Shirt http://www.foxnews.com/us/2013/04/23/dad-west-virginia-boy-arrested-over-nra-shirt-says-hell-fight-punishment/

7. Preston, Peter (February 18, 2001). "Six million and counting". *The Observer* (ardian.co.uk). Retrieved June 14, 2001.

8. IBM and the Holocaust http://en.wikipedia.org/wiki/IBM_and_the_Holocaust#cite_note-Preston2001-1

9. Mac users steered towards higher priced rooms. *Wall Street Journal*

http://online.wsj.com/article/SB10001424052702304458604577488822667325882.html

10. Insurers Consider Computer Profiles

http://online.wsj.com/article/SB10001424052748704648604575620750998072986.html

12. IRS publishes SSN to Public website.

http://now.msn.com/irs-publishes-social-security-numbers-by-accident-when-uploading-data

13. 22 Federal Agencies Who Joined The Department of Homeland Security in 2002. http://www.dhs.gov/who-joined-dhs

14. Lockheed Martin is shadowing you.

http://www.counterpunch.org/2011/01/11/is-lockheed-martin-shadowing-you/

RESOURCES

Ten Ways to Protect Your Privacy While Entering Facebook Contests

(http://contests.about.com/od/facebookcontests/tp/10-Ways-To-Protect-Your-Privacy-While-Entering-Facebook-Sweepstakes.htm)

The Kim Komando Show Internet Radio Show and Website for Privacy and other Computer Questions (free and membership) (Komando.com)

Electronic Frontier Foundation (https://www.eff.org/about)

The Electronic Frontier Foundation (EFF) is the first line of defense against invasion of your electronic or digital privacy. EFF broke new ground when it was founded in 1990—well before the Internet was on most people's radar—and it continues to confront cutting-edge issues defending free speech, privacy, innovation, and consumer rights today. From the beginning, EFF has championed the public interest in every critical battle affecting digital rights.

JJ Luna: How to Become Invisible http://www.jjluna.com/