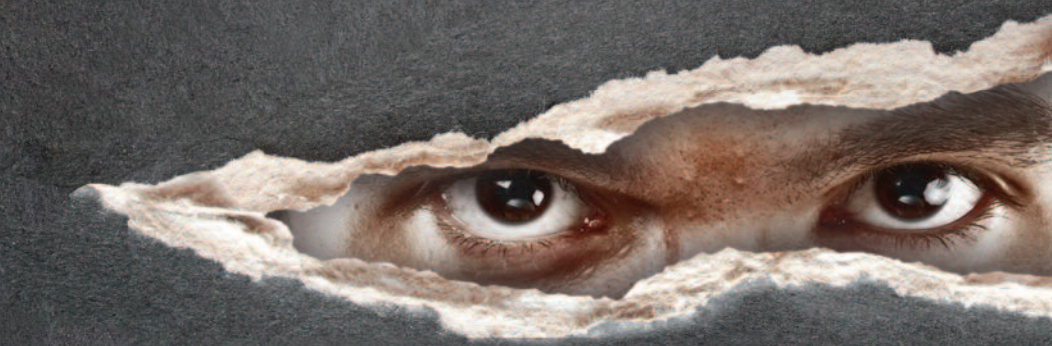
A SURVIVAL TREASURY

THE ULTIMATE PRIVACY GUIDE:

Simple, But Effective Strategies for Making Big Business and Big Government BUTT OUT of Your Personal Life!



By Bob Livingston
Founder, *Personal Liberty Alerts*™
Editor, *The Bob Livingston Letter*™

A SURVIVAL TREASURY

The Ultimate Privacy Guide:

Simple, But Effective Strategies for Making Big Business and Big Government BUTT OUT of Your Personal Life!

Copyright © 2012 *The Bob Livingston Letter*™
All rights reserved.

The information contained in this book is meant to educate the reader, and is in no way intended to provide medical, financial, legal or any other services for individual problems or circumstances. We encourage readers to seek advice from competent professionals for personal health, financial and legal needs.

This information is published under the First Amendment of the Constitution of the United States, which guarantees the right to discuss openly and freely all matters of public concern and to express viewpoints, no matter how controversial or unaccepted they may be. Any references for additional information that we may provide are for the reader's benefit only and are not affiliated with *The Bob Livingston Letter*™ in any way, unless otherwise stated. All information is believed to be correct, but its accuracy cannot be guaranteed. The owner, publisher and editor are not responsible for errors and omissions.

Published by *The Bob Livingston Letter*™
P.O. Box 1105, Cullman, AL 35056

www.BobLivingstonLetter.com
www.PersonalLiberty.com

A SURVIVAL TREASURY

The Ultimate Privacy Guide:

Simple, But Effective Strategies for Making Big Business and Big Government BUTT OUT of Your Personal Life!

Contents

Chapter 1:
Big Brother IS Watching 11

Chapter 2:
Privacy Basics: Keeping a Low
Profile in a Facebook World 29

Chapter 3:
Banking In Secret in the Post-9/11 Era 59

Chapter 4:
How to Keep Your Home Private and Secure 89

Chapter 5:
How to Be Secure While Traveling 105

Chapter 6:
Maintaining Your Medical Privacy in an
Obamacare World 115

Chapter 7:
Putting the Genie Back in the Bottle… Sort of 125

References 141

Bibliography 143

Index 145

Introduction

Privacy is something people have traditionally taken for granted. They generally assumed that no one had access to their private information, financial transactions and daily activities. But we live in a world where political decisions and technological advancements mean you live in a fishbowl. This has made it easy for government snoops, law enforcement investigators, private detectives and even people with ill intent to dig deeply into areas that once were off limits. Unless you take active steps to protect yourself, you have no privacy anymore.

Some people don't take privacy seriously because, they say, they have nothing to hide. They're suspicious of those who are concerned about privacy, believing it must mean someone is covering up something they've done wrong. Many police and government officials feel that way as well, so they don't understand why we care.

But wanting to maintain privacy doesn't have to imply that you are behaving nefariously. There are many people who simply want to steal what's yours. There are vindictive spouses or aggrieved business partners out for revenge—and perhaps some of your wealth. There are government snoops and private detectives who may not even be looking for you, but for someone you may know. For all of these reasons… and for many more… you should take seriously the risks everyone is exposed to in this information-saturate world.

Did you know that you could be a criminal and not even know it? In his book, *Three Felonies a Day: How the Feds Target the Innocent*, Harvey Silverglate shows how a huge volume of overly broad and vague Federal statutes have essentially criminalized almost every behavior. He says there are 4,450 listed criminal Federal offenses and additional Federal codes for Federal attorneys to employ to entrap anyone they choose to target.

Silverglate believes that the average American violates three of these laws each day. "Even the most intelligent and informed citizen (including lawyers and judges) cannot predict with any reasonable assurance whether a wide range of seemingly ordinary activities might be regarded by federal prosecutors as felonies," Silverglate writes.

So having violated a law you didn't know existed, and then having a chance encounter with an overzealous police officer or prosecutor could set you up for a world of trouble that is expensive to defend against; or maybe set you up for some time behind bars.

And then there are the myriad of regulations constantly being revised and added to by bureaucrats in the various alphabet soup regulatory agencies of the Federal government. Virginia farmer Joel Salatin, in his book, *Everything I Want to do is Illegal,* believes there is no way for the American farmer to not run afoul of some bureaucrat's interpretation of a Federal code or statute.

Today there are pages of news reports of government bureaucrats imposing harsh penalties and fines on everything from children raising rabbits or selling lemonade to people growing the wrong type of shrub in their yard or just letting their grass get too high. And often these people not only had no idea they were breaking a law. In many cases the

enforcer would not have known either had not a child or homeowner let the enforcer onto the property or answered a few innocent-seeming questions.

For some people, though, it's simple and obvious why we care about personal privacy. For us, privacy is tightly linked with the individual freedom to do and be what we want. It's a part of our natural rights and we don't apologize for standing up for what's ours.

If you're one of those people, this book is for you.

CHAPTER 1

Big Brother IS Watching

In George Orwell's 1949 book, *1984,* there's an all-pervasive, dictatorial government that sees everything. The regime's leader is an enigmatic figure called, "Big Brother." His picture is everywhere and the people are cowed into submission by constantly being reminded, "Big Brother is watching you."

There are "telescreens" everywhere, and Big Brother watches everyone through those telescreens. This book was science fiction when Orwell wrote it, because the technology didn't exist for the kind of surveillance he envisioned. But that technology does exist today. It's not as simple and obvious as screens through which someone is constantly watching. It's far more subtle than that. Instead of reminding you that he's there, Big Brother has inserted himself into the hidden nooks and crannies of your life from which to secretly observe you.

The first thing to be clear about is that Big Brother is, indeed, watching you. The Federal government is devoting more resources than ever to keeping tabs on us. The surveillance is justified in the name of fighting terrorism, fighting crime and catching tax cheats. Whether you believe those justifications or not, the implications for privacy are staggering.

The U.S. government routinely monitors every bit of electronic communication on Earth today. Echelon is the common name for the vast electronic monitoring system

operated by the Federal government, in collaboration with the governments of Canada, Australia, New Zealand and Great Britain. This network monitors satellite links and other major hubs of communication to listen in on telephone calls, faxes, email and other data traffic. Your communication is being monitored silently, without you ever realizing what's going on.

Carnivore is the name of a software package that the government started using as far back as 1997 to monitor Internet traffic. Although the original custom software was replaced in 2005 with a more advanced commercially available system, its capabilities—by any name—are chilling. It sucks in Internet data and "listens" for things the government wants to know.

Sometime in the 1960s, the U.S. government learned that computers and certain other electronic devices, particularly those that transmit data through wires, emitted electromagnetic data. So it began a program to determine whether that data could be deciphered into something intelligible. It named the program Telecommunications Electronics Material Protected from Emanating Spurious Transmission or Tempest.

Researchers learned the EMR that is emitted contains, to varying degrees, the information that the device is displaying, creating, storing or transmitting. With the correct equipment and techniques, it is possible to reconstruct all or a substantial portion of that data. Some computers and devices are far more susceptible than others. For example, some US Robotics data/fax modems generate incredibly strong EMRs when active, which can be read even by comparatively crude equipment. Wireless handsets and office speakerphones are other devices that generate extremely strong EMR signals.

The range in which an eavesdropper can monitor emanations varies tremendously according to conditions. In most cases,

the emanations can be picked up with proper equipment from a distance of around 200-300 meters. However, in some cases where a signal has been captured by a conductive medium (such as a power line), monitoring can occur over a distance of many kilometers.

Monitoring devices include various kinds of sensitive receivers, which can monitor a wide range of frequencies, and a combination of hardware and software that is capable of processing the received signals into the original data. The data that is picked up is often corrupted by such things as external EMR interference, signal weakness over distances and partial transmission. Advanced algorithms can help provide a more complete picture of the original information.

Equipment shielded from Tempest is only available to government entities. But there is nothing to prevent you from shielding your own equipment.



Shielding of devices from EMR is achieved by a number of methods. The most sophisticated devices use advanced micro-components that have been designed from scratch to minimize Tempest emanations. Generally, shielding involves enclosing the device in a Faraday cage that does not permit stray emanations, along with special modifications to the power source. This usually involves a heavy metal case around an object. Tempest shielding also requires the proper design of a room and placement of equipment within it, to ensure that no information can escape.

For individuals who wish to be more secure against Van Eck phreaking—the process of eavesdropping on the contents of electronic transmissions by detecting EMRs—but cannot invest in this level of equipment, some software products recommend special displays that limit the effectiveness of monitoring of emanations from a CRT monitor.[1]

It's not just your electronic communication that's at risk. Every financial transaction goes through sophisticated monitoring. Every time you swipe your credit card, take money out of your bank account or transfer money to another account, there are computers keeping track—and those systems report anything out of the ordinary to the government, all in the name of fighting "money laundering."

Governments even keep tabs on your public movements and, police departments around the country have installed scanners that can automatically and instantly read every license plate that comes within their sight. That information is logged in police databases, slowly building a collection of information about who has been where. Until the U.S. Supreme Court struck it down as illegal, police agencies were even attaching GPS tracking devices to cars without court orders.

More and more, there are video cameras and even microphones recording what goes on in public. Police are also now employing the same technology used in the airport naked body scanners—backscatter radar—in vans and trucks. These are used to peer inside homes and even passing vehicles

And with computer technology slowing tying all of these technologies together, the things that would have been pure science fiction just a few years ago are now the nightmare scenario of political fact in a country where privacy is not longer respected by our government entities.

Corporate Surveillance and Data Mining

It's not just governments that are tracking you, though. Your information is worth big money to various corporations. For instance, Google makes its money through advertising that matches the things you search for online. The company keeps huge databases that records what users have searched for. These aren't simply databases of all searches joined together, but rather databases that show who searched for what and when.

If you use any of Google's services, the company keeps a record of what you do across its other services. If you're searching for information about hiding assets or tax avoidance, Google knows about it. If you watch YouTube videos, Google knows that, too, since it owns YouTube. It can track what you've watched and match it with what you've searched for. The purpose is to present ads for products it thinks you might be interested in.

But possibly the worst offender among Google's products is Gmail. If you use Gmail, Google's software scans your messages and looks for keywords. Those keywords are then used to present advertising that it believes might be relevant to you.

It's easy to see why Google wants the information—and it's easy to see why advertisers want access to the information as well—but anyone can see where it can easily lead. If Google knows you've been searching for information about tax avoidance or moving assets overseas, that information might very well make its way into government computers. Today, getting that information still requires simple legal steps for the government, but it's a short hop to simply linking the systems and allowing law enforcement and various bureaucrats to have real-time access to what you're doing online.

And it's not just Google that you need to worry about. Facebook is doing the same thing, but it has its hooks even deeper into your online activities than Google does. Facebook computers know who your friends are and who you interact with. They know where you've been and what you're talking about. They contain pictures of you, whether you posted them or someone else did. In other words, those computer servers have a copy of your digital life on them—and that information is being stored forever.



If a company such as Google or Facebook offers you a service, it's not because they're just such nice people. They only offer you "free" services if they can make money from them. So if you're not paying for a service, you can usually count on the fact that you—and information about you—are the "product" being sold by the company.

This information is worth money to Google and Facebook, among other companies, because many companies are willing to pay to target advertising at just the right group of people. Since the online services you use know who you are, where you live, what you talk about and what you search for, they can do a pretty good job of predicting other things about you. That ability allows them to sell access to you to many companies.

As bad as this data collection might be, it's at least legal and the companies claim they're taking steps to protect your privacy. Even if you believe them, though, the information is in databases just waiting for governments to demand access to it. Even if it takes a court-ordered warrant right now to get access to it, how long is it going to be before the databases are linked automatically? By the time you find out that Big Brother has real-time access to all of your digital life, it will be too late to do a single thing about it.

Biometric Scanning and Identity Cards

Across the country, there are growing databases of DNA information about more and more Americans. In some cases, the Federal government collects the information and in others it's State government. By 2009, the Federal government had collected DNA profiles of 6.7 million people, mostly convicted criminals. But that program is expanding. At the time, the database was growing by only about 80,000 entries per year,

but it's now growing by more than a million a year.

Although this DNA data collection started with just convicted criminals, it's been expanded to include people simply arrested, many of whom will have charges dropped or be found innocent at trials. Just from having been arrested, though, their DNA is forever in a government database.

In 35 States, even children who face juvenile convictions have DNA samples taken. In another 16 States, DNA samples are even taken for those convicted of misdemeanors. That means if you write a bad check by accident, your DNA could end up in a permanent criminal DNA database.

It's bad enough when it's criminals and possible criminals —and you might be willing to ignore the privacy rights of those who have been arrested—but what about newborn babies? In many States, DNA is taken and put into State databases without the parents' permission or even knowledge.

Mandatory State testing of newborns for various diseases started in the 1960s, but it's greatly expanded since then. Some States automatically test for possible health issues that can only be diagnosed through DNA tests and insurance companies are required to pay for those tests. Because the insurance company pays for the tests, the company gets the results—and those results are on a child's permanent health record. This can affect the cost of care in the future if a company decides that some genetic marker is a bad risk for some reason.

But it's not just insurance companies that have access to this information. The DNA is routinely made available to researchers for a variety of reasons. In some cases, the names are still attached to the DNA samples. Parents are supposed to be required to give consent when the names are attached to the data, but no one really has any way to enforce that—

especially if you never even knew the samples were taken.

In Texas and Minnesota, there's a State form you can fill out to ask that the State delete your child's information from its database. In others, though, you don't have any real options. You can request that the DNA sample be deleted from the database, but the State isn't under any obligation to honor your request.

What's more, you might be required to have your DNA in a database in the future just to have a job. In the name of fighting illegal immigration, many politicians want a system that would require every U.S. worker to have an identity card with biometric information embedded into it. That might be DNA or iris scans or simply fingerprints. But we're close to the day when every person will be required to hold a government-issued identity card just to have the right to work.

When that happens, how much easier is it going to be for government agencies—including the IRS—to closely match every penny of income that you have? If you're not in the database, you won't be allowed to work. If you're in the database, everything about you is available to government agencies. And as those government databases are increasingly linked between agencies and different levels of government, it's going to be harder and harder to keep anything private.

Making All Businesses Government Spies

Many of the companies you do business with have been turned into government spies. Even though you're the one paying the company and you're the one who has a business relationship with it, governments require those companies to put their needs and desires ahead of yours.

The most obvious example is any company in the financial

sector. Your bank or broker isn't your friend. Even if the people at the company want to be loyal to you, they're required by law to report what you're doing to government agencies—and they're not even allowed to tell you when they do it.

The Financial Crimes Enforcement Network (FinCEN) was established in 1990 by order of the Secretary of the Treasury. It wasn't that big a deal at first. But as new responsibilities and powers were given to the bureau, it became a very big deal.

Banks have long been required to file currency transaction reports when individuals deal in cash. Governments want to be able to track money. Since cash is harder to track, government agencies want to be notified so they can look into cases in which people deposit or withdraw large sums of cash. But with the passage of the USA PATRIOT Act in 2001, the government has greatly stepped up its snooping into your financial affairs.

The USA PATRIOT Act required FinCEN to establish a secure network that allows the agency to keep tabs on what anyone is doing at any of the 27,000 financial institutions in the U.S. This sinister system allows government snoops to have real-time access to your information and to what you're doing. If you're on their radar screen, they can know everything you're doing. Your information is identified, centralized and then evaluated by various agencies in law enforcement.

And what if you'd rather keep your financial transactions secret? One of your few options is using U.S. Postal Service money orders. The post office doesn't require identification for money orders of less than $500.

It's not just banks that have become government spies,

though. Telecommunications companies have been enlisted in the war against your privacy, too. The passage of the Communications Assistance for Law Enforcement Act (CALEA) in 1994 was a huge step toward making the nation's phone systems a big government wiretapping operation.

CALEA requires telephone companies to modify their equipment to make it easy for government agencies to wiretap telephone calls and VoIP calls (such as Skype) as well as all other broadband Internet traffic—all without a warrant. It's even illegal for the company to tell you that your information is being monitored.

USA Today reported in 2006 that the major telephone companies were cooperating with the National Security Agency (NSA) to monitor the phone records of everyone in the country. The NSA maintains a call database with all of this information, so it knows who you talk to.

Traffic Cameras and Surveillance Drones

After the terrorist attacks on New York City and Washington, D.C., on Sept. 11, 2001, we started to see changes in official attitudes in this country toward public surveillance. While some world cities such as London have long been covered with video cameras, this country had escaped that to a large degree. With the horror of terrorism as an excuse, that changed rapidly.

In many cities, there are cameras in more and more places. There are an estimated 30 million surveillance cameras in this country and they record approximately 4 billion hours of video each week. Some of those are traffic cameras and are supposed to help in the management of traffic signals. But the increasing sophistication of the cameras means that

they're coming to be useful for identifying specific vehicles as well. So even if you believe you're driving on a public highway far from watching eyes, there might be a camera monitoring what you're doing.

Then there are the street-level cameras that send images of people all around a city to a police command center. The cameras are sometimes equipped with microphones as well, so police can choose to listen in to what's being said. These cameras have been installed all over cities such as Washington, D.C., that were considered possible terror targets, but they're increasingly being used on random public streets where terrorism was never a realistic threat—and politicians and bureaucrats aren't going to let the lack of credible threat keep them from taking greater control.

Another type of public camera that's increasingly being used is the so-called "red light camera," which photographs cars that didn't make it through a yellow light in time. Government officials claim the cameras are all about public safety, but critics contend that they're really about revenue for cities and counties.



At least you know that cameras such as these are generally limited to public spaces, but what about when you're on your own property, far from the public view? You're not even safe there, because government agencies are using surveillance drones to watch what they want to see on private property.

These small unmanned air craft are quiet and aren't likely to even be noticed, but they can see what you're doing because they're equipped with high-powered cameras and transmitters to send video back to police or other agencies.

A North Dakota man is the first to be convicted of a crime using evidence obtained by a Predator drone. (That's the same kind that the government uses to kill suspected terrorists in other countries.) He's an anti-government sort who lives on a 3,000-acre ranch and wants to be left alone. But when there was a dispute about six cows that he found on his property, the local sheriff's department called in a drone to pinpoint his exact location on his property before sending a SWAT team to storm the place.

Police departments around the country are starting to buy the drones and they're justifying them in a variety of ways, using everything from the threat of terrorism to the desire to see what's going on in hostage situations and even to having better vision of what's happening inside forest fires.

Recent changes in the law mean that drones are going to become very common in U.S. skies, so be prepared, regardless of how remote your property or how big your spread is. According to the Federal Aviation Administration, there will be somewhere in the neighborhood of 30,000 of the unmanned drones over American skies by 2020. Some of the "eyes" aboard those drones might very well be directed at you very soon.

DNA Required for High School Tests

A very small percentage of high school students attempt to cheat on college entrance tests such as the Scholastic Aptitude Test (SAT) or (ACT) originally called the American College Test. In order to combat that small instance of cheating, officials are developing a "digitalDNA" card that students will be required to show to take such tests.

Instead of coming up with a plan to deal with the very few cheaters, the system will now require every student taking such a college entrance test to put his or her DNA into a database. What will happen to that DNA? Nobody's saying yet, but it's a good bet that the use of the data will be expanded over time.

You might notice that in each case of identification such as this, the original system is supposed to be designed for a very specific purpose, but the purpose is expanded over time, eventually leading to cases in which more information is being collected than would have been tolerated in the beginning.

Right now, it might sound reasonable to require such an ID card to take a college entrance test, but what about when that card is extended to the use of colleges themselves? Why would they not want the cards to make sure the people taking tests are who they say they are? And what happens when some politician gets the bright idea to link the databases for college kids with the job ID databases required to have jobs? And why not cross-link those to medical records and credit records and housing records?

The problem with something such as this digitalDNA card isn't that we want people to cheat on tests. The problem is that it's another piece of a vast web of databases that contain all of our lives. And as those databases grow, they are going to be linked. It's a true nightmare scenario where any bureaucrat has access to anything he wants to know.

States Want to Track Every Website You Visit

Early in 2012, a State legislator in Hawaii introduced a bill that would have tracked every visit to every website by every Internet user in the State. It would have required Internet service providers (ISPs) to keep "Internet destination history information" and the user's name and address for two years.

After a firestorm of national controversy, the bill was withdrawn, but Hawaii State Rep. John Mizuno plans to introduce the bill again next year.

On the national level, there have been plans that would do similar things, although none of them were quite as far-reaching as the one in Hawaii. For instance, in 2011, a U.S. House committee approved a measure that would have required ISPs to keep records of what their customers do online for a year.

In order to make the plan more difficult to oppose, proponents of the data retention requirements called the bill



the Protecting Children From Internet Pornographers Act of 2011. The reasonable-sounding name—after all, what normal person doesn't want to protect children from online predators?—is only used to make the bill more palatable because the information would have been available to police for any investigation. Many believed that the information would have been available to private parties such as attorneys in civil disputes such as divorce, insurance fraud and other cases.

Keeping this information isn't just a partisan issue for one party or the other. Both Democratic and Republican administrations have favored data retention for more than a decade, and the concept has been endorsed by the Department of Justice and various police groups.

Fortunately, public outcry killed the legislation in 2011, but it will be back. Too many government agencies want access to your information for them to give up. They're going to keep asking for these laws until they get the power they want.

Feds Want to Make Using Fake Names On the Internet a Felony

Many Federal officials and other law enforcement agencies want to make it a crime to use fake names online. Instead of just pursuing a law that would make that illegal, they've taken the approach of broadly interpreting existing laws.

The Computer Fraud and Abuse Act was passed in 1986 to deal with malicious computer hackers who broke into online servers. Over the years, though, the law has been expanded beyond its original intent. Today, prosecutors have come up with novel interpretations of the law in order to legally go after people they don't like.

For instance, the law criminalizes any computer use that "exceeds authorized access," but what does that mean? When the law was passed, it was understood to apply to those electronically breaking into computers remotely. Now, though, officials have claimed that if you violate the "terms of use" posted on a computer website, you're guilty of a crime.

For instance, when prosecutors wanted to go after a woman they disapproved of otherwise, they couldn't find any law she had broken, but they found she had set up a MySpace profile using a fake name. MySpace was a popular social networking site at the time and its terms of use required users to create accounts using real names. So prosecutors charged her with conspiracy to violate the Computer Fraud and Abuse Act. She was found not guilty, but the precedent is set for bringing such prosecution.

Under this absurd reading of the law, it would be illegal to visit any website if the site posted rules banning certain people. The Democratic Party could post rules banning Republicans from visiting its site. Companies could post rules banning its competitors from visiting. (One company actually tried that and filed a civil lawsuit when a competitor simply visited its website.)

Up until now, Federal prosecutors didn't bring many of these cases because they were classified as misdemeanors. But in late 2011, the Obama administration proposed that violating this law be made a felony. Although the proposal hasn't passed yet, it's still a goal for politicians and bureaucrats who want more control.

If that happens, it will be yet another way to selectively control Americans—by prosecuting those who are targeted and ignoring the rest.

CHAPTER 2

Privacy Basics: Keeping a Low Profile in a Facebook World

Every keyboard stroke a person makes while connected to the Internet leaves a digital trail as identifiable as tracks in fresh snow. Every credit card transaction and every savings or value card used leaves a digital fingerprint for marketers—or the government—to add to the dossier they're compiling on your spending, travel and eating habits. Almost every move you make tells someone something about you. Is that what you want?

What Facebook Really Knows About You

If you use Facebook and similar social networking sites, you need to understand that those sites are in business to sell your information.

Facebook isn't providing a service to you out of the goodness of Mark Zuckerberg's heart. The company provides a "free" site where you can tell your friends and family what you're doing because they can sell that information to advertisers. In general, if you're not paying for a service, the product that the company is really selling is you.

But Facebook has "privacy settings," you might think. Surely that's enough to protect you from others finding out things you post about yourself, isn't it?

No, not really. First, you have to remember that Facebook is ultimately just a website. Anything that's online can be accessed by anybody else online if he knows how to get to it. Facebook and other sites say they're secure because they limit access to people with certain other Facebook accounts. But how secure is that?

There have been numerous examples of programming mistakes at Facebook and other companies exposing personal information by mistake. Even if a company's intentions are perfectly good, you're at the mercy of how effective they are at protecting your information. Your privacy isn't their top priority. Finding out more about you and selling that information to advertisers is their top priority. So if there are programming glitches that allow information to leak out, they'll eventually be fixed. In the meantime, your information isn't secure.



Another way that people can get access to your Facebook information is through what's referred to as "social engineering." It's a term for practices that don't use technical avenues to hack in,

but rather rely on tricking you. There are many ways to do that.

The most common way for people to gain access to your account is to pretend to be people they're not. In Missouri, a high school principal was forced to resign after she invented a student name on Facebook and then sent "friend requests" to many students at the school. She was trying to keep tabs on a controversial issue at the school, so she pretended to be a student in order to read the pages of those whose pages would otherwise be blocked to her.

This goes on far more frequently than you think. People trying to learn about others can sometimes send friend requests to other people on a person's "friend list." After becoming Facebook friends with some of those people, the fraudulent account sends a request to the actual target of the attack. The victim sees that the person is "friends" with other people he knows, so he assumes he knows him and accepts the request. By doing that, the victim has given the attacker full access to whatever information he posts.

Even if you're able to keep your Facebook friends limited to people who truly know you, you're at the mercy of the care (or lack of care) they take to keep their own login credentials secure. If one of your friends uses an easy-to-guess password, someone else can log into that person's account and see your information. Anything personal and private that you've posted is then available to him.

But what if you only post things that you don't mind being in the public domain? What if you don't post personal information or embarrassing pictures? There's still something you need to be concerned about if you don't want people to know certain things about you.

First, Facebook knows where you are. Every time you log on, the company knows the location of your computer because of the Internet Protocol (IP) address, which is the numerical code that the Internet uses to route information to the proper place. In most cases, an IP address tells Facebook where you are. It doesn't give an exact location, but it's close enough to know what city you're in and even what part of a city, in many cases.

But it's not just your posts you need to be concerned about. The company has created scanning software that monitors chats for words or phrases that signal possible wrongdoing including discussions about criminal behavior, exchange of personal information or vulgar language. It then turns these suspect conversations over to law enforcement for evaluation.

Facebook apparently believes it is performing a public service by doing this. And there is no denying that some good has been accomplished. The company recently cooperated with the Boston Police Department by sending wall posts, photos and login/IP data of a murder suspect.[2] It also touts that that it assisted the FBI with tracking down a sexual predator who had targeted a 13-year-old Florida girl.[3]

But privacy experts fear the company's monitoring activities go too far and the impersonal technology that is unable to discern the context of conversations may lead to innocent people being ensnared in costly investigations by overzealous police investigators and district attorneys.

Your Social Security Number And Date of Birth

Your Social Security number and date of birth are something like a golden ticket that provides access to a lot of

information about you. Because it's insanely easy to get that information, it's shocking how often the number is used to identify us and to associate information with us. The worst thing is that having access to information about us like this can allow us to become targets for insane people.

In 1999, Liam Youens used a company called Docusearch to get the Social Security number and work address of a woman named Amy Boyer. Youens had developed a crush on Boyer when the two were in eighth grade together. He never told her, but he imagined himself as a rejected suitor. Over the years, he periodically believed he loved Boyer and then hated her at different times.

A few months after buying the information about Boyer, Youens drove to her workplace and killed her. Then he committed suicide. Without the information that Youens bought from the online information broker, Boyer might very well be alive today. Do you think it's worth exposing yourself to the kind of fate that befell Amy Boyer?

Even the Social Security Administration recommends that you be careful about who you give your Social Security number to. The agency says you should ask why the number is needed and what will happen if you don't give it. In many cases, companies will assign other identification numbers to people who decline to provide their Social Security numbers. There's just no reason to have your number in too many computer databases.

What can you do if someone has stolen your identity using your number? In some cases, you can actually get the Social Security Administration to issue a new number for you. Ask for a Social Security Administration document called "Your Social Security Number and Card"

(Publication No. 05-10002) to find more information about the circumstances under which you can get a new number. You'll need to be able to prove that someone else is using your number in a way that harms you.

Your Driver's License

Did you know that many States sell driver's license data, including your photograph? Few people do.

Your personal data, like your height, weight, age and home address is routinely sold to marketers and "welcome wagon-type" companies. But a company named Image Data is also buying driver's license photos. And the frightening thing is the source of funding Image Data uses for purchasing these photos is the U.S. Secret Service.

What the Secret Service wants with these photos is anybody's guess. Image Data claimed it was for a program that would match your driver's license to their computer database when presenting checks for cashing—all in the name of protecting your accounts, of course.

For this reason, privacy experts recommend you use other forms of ID when possible. And in most instances it is. In fact, the only time you must produce a driver's license for identification is during a traffic stop.

A better alternative for a photo ID is your passport. It doesn't contain as much personal information as a driver's license but is acceptable as a form of photo identification.

The Internet is Forever… Sort of

If information about you ever gets posted on the Internet, there's a very good chance that someone can find it later, even if you do everything you can think of to delete it.

That's because once information is stored in digital code, it's easy to copy, so that means that someone has probably made a copy of the page that had information about you.

For instance, have you heard of the Wayback Machine, which is run by the Internet Archives? You can go to a website *(http://archive.org/)* and enter the name of almost any other site, even some small personal sites. There's a good chance you'll find an archive of at least some old versions of that website.

Although it might just seem like fun trivia to find old versions of websites for *CNN* or some major website, there's an equally good chance that there's something about you that has been written or said at some point. In the old days, copying and storing information was time-consuming and expensive. Today, it's easy, automated and cheap.

Be careful about what you post about yourself online. If it's something that could damage you if someone else saw it, don't post it. Don't assume you can delete it later and no one will see. In many cases, the things you post are there forever for all the world to see—and you'll have absolutely no control of those things once someone else has made a copy.

Here's an example of how that can come back to haunt you. In this case, the information helped to stop what might have been fraud, but in other cases, it might be used against you instead. In the New York court case of *Kathleen Romano v Steelcase Inc.,* the plaintiff claimed that an office chair collapsed and caused her pain, health problems and $200,000 of spinal surgery. She claimed she had been mostly house-bound and was unable to enjoy life, but what the defendant said and the picture she painted of herself on Facebook and MySpace told an entirely different story—showing photos of Romano enjoying trips to Florida and Pennsylvania.

The court required Facebook and MySpace to produce all of the information from her account. The most interesting thing, though, is that the companies were required to produce pictures and information that Romano had deleted from her profile, showing conclusively that these companies retain your information in their archives even after you believe you've deleted it. In some cases, such information might only be held for 90 days or so after you've deleted it. In other cases, the information might remain on some backup drive buried in the archives of a company's data center. The point is that if you don't have real control over your data after you've posted it.

Tracking Codes are on Everything

You see bar codes everywhere you go today. The vast majority of products sold in stores have scannable UPC codes. You're also starting to see QR codes that you can scan with your smartphone. Your mail comes with bar codes beneath the address and it has your information embedded in code that the post office's scanners can read. The same is true for packages from UPS or FedEx. When you sign for a package at the door, the courier scans a bar code and the information goes into a computer. It seems that these bar codes are everywhere.

But those aren't the only codes that track things today. Much tracking is invisible to you. For instance, some color laser printers embed a code in each sheet that you print. Even though you can't see it with the naked eye, your printer identifies which printer produced the sheet, along with the date and time of the printing. Some of them even contain more information. In the case of the printers, the excuse is

to fight against counterfeiting paper currency, but do you have any question that governments would prefer if this were true of every printer?

Have you ever noticed that certain web pages have exceptionally long URLs? In many cases today, that information isn't just the location of the page. It can also identify where you found the link and possibly even identify you. So when you share links with others, they might point back to you in ways you might be surprised about. The source of a web page isn't typically going to be a problem, but it's just an example of how easy it is for tracking to occur that you're unaware of.

A type of tracking with much greater long-term privacy concerns involves the use of RFID chips (RFID stands for radio frequency identification). An RFID chip is a tiny object—about the size of a grain of rice—that can be attached to a product (or other object) in order to track it. The scanner doesn't have to come close to the chip to read it. Instead, the scanner just has to be within a few feet of the chip in order to read the information.



There are many beneficial uses of RFID technology. For instance, an automaker can attach RFID chips to each car in production and monitor the state of an entire factory's production without having to set foot on the factory floor. A maker of a product being shipped to retail stores can attach a cheap RFID chip to each box going to a store and then know for certain when that box has been received. Companies around the world are using this technology and are saving money by having instant access to information about their inventory that was otherwise inaccessible or expensive to collect.

But what about when this same technology starts tracking you? Is this a good thing? Or do you become just another product that someone believes he owns?

The U.S. government now embeds an RFID chip into all U.S. passports. That means that anyone with a scanner capable of reading the code is theoretically capable of reading your passport information if you just walk nearby. The information might be encrypted, but any encryption can be broken. What is the necessity of having your information available in a form that can be picked up by any determined person who wants to know? The government has never given us a believable explanation for why this is necessary.

These chips can be implanted into various products that we buy, and many privacy researchers believe it will be possible to figure out who you are from matching the ID codes in the RFID chip with credit card records. And all of that could take place without you ever knowing that you or your possessions were scanned.

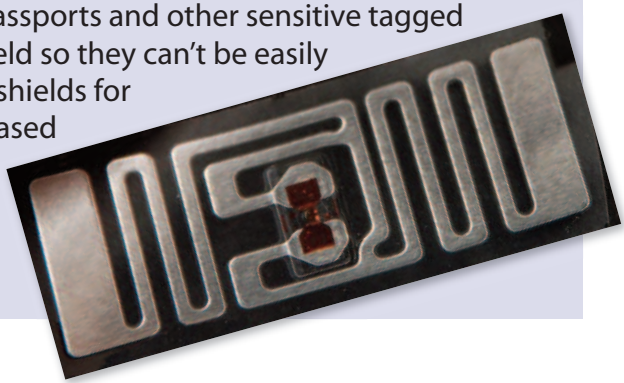
To make things even worse, the U.S. Food and Drug Administration has approved the use of RFID chips in human beings. This technology has been used to track the

RFID Countermeasures

Because of the potential danger to your privacy that RFID tags represent, you need to consider what you can do about them.

First, try to avoid any products that have the tags built into them. This is difficult because manufacturers have long ignored the privacy concerns expressed by consumers. Other tips include:

- When possible, purchase products that have the tags in the packaging rather than the product.
- Pay for RFID products with cash rather than a credit or debit card or bank check, since these can link data about you to the tag.
- Avoid using discount store cards and loyalty cards that will be linked to the products you buy.
- When possible, buy or use older or second-hand products that lack RFID tags or have tags linked to someone else.
- Have older clothing, shoes and other products available for use that are RFID free for those times you wish to travel unchecked.
- Learn to recognize RFID tags and try and discover ways to remove them without destroying the product.
- If they are available, employ blocker tags to limit the information that can be gleaned from RFID tags.
- Be cautious about tagging pets with a similar system, since that would tag everyone associated with the animal.
- Carry credit cards, passports and other sensitive tagged documents in a shield so they can't be easily read. "Faraday Box" shields for these can be purchased or constructed.



Source: Long, *Protect Your Privacy,* p. 218.



ownership of some pets for years, but it has far greater implications for humans. For instance, there are proposals to implant a person's medical records in a chip and implant it. Although this would give instant access to someone's medical records in an emergency, it also makes your medical records available to anyone with a scanner and the ability to break the encryption.

These human implants can also be used for access to buildings or even for paying bills. The VeriChip Corp. is marketing a system that uses implanted chips to control who is allowed into certain places. As systems such as this become popular, we have the real possibility of it becoming the de facto standard. As more and more people accept the system, those who refuse to be "chipped" would be locked out of many jobs. It will be a world where those who were concerned about their privacy could be second-class citizens because they didn't want the chip.

And the worst part is that as more and more people accept the technology—and accept the chips being implanted into people—we're looking at a day in the future when a majority

will insist that everyone use them. That's why it's important to pay attention to the technology and its implications, now, before it's too late.

Your Car's Black Box is Spying on You

They're officially called "event data recorders," but we all know them as black boxes. They're the devices in airplanes that records everything going on and then provides information in the event of a crash. If you have a car made in the last decade or so, though, you might already have a black box recording information about you.

If you don't have a black box in your car yet, you will before long. Politicians have been pushing for making black boxes mandatory on all new cars. One such proposal would mandate black boxes for every new car beginning in 2015. As fast as the privacy landscape is changing, it might very well be law by the time you read this.

Some of these devices record what you're doing all of the time, but others only record when they detect that there's something similar to an accident going on. The question that no one is clear about yet is who owns that data and has access to it.

If you own the device and the data, no one would have access to it without your consent. But the intention is for police and courts to be able to access the information routinely as a part of investigations and court cases. In the future, expect insurance companies to routinely have access to this information, too. That might not sound so bad, but what if those insurance companies use the data about how you drive to jack up your insurance rates? What if you have no accidents, but a bureaucrat at your insurance company can remotely look at your driving habits and decide he doesn't approve?

The technical details are still being worked out, but the proposal mentioned earlier about mandating black boxes for all cars by 2015 would also set up an infrastructure to allow roadside sensors to remotely read cars' black boxes. In this way, your driving could be monitored remotely—how fast you drive, how you brake, where you drive and many other things. Some long-range proposals call for taxing drivers for every mile they drive (California is actively considering this), based on the information coming from the black boxes.

The privacy implications are enormous. Imagine not being able to travel anywhere in your own car without your movements being recorded by the car and then transmitted to government agencies and possibly insurance companies. In such a world, they won't have to ask for your "papers," because they'll already know where you've driven in the past and where you're coming from today without asking you a thing.

Some privacy advocates have called for a strict limitation on this data collection. They've suggested that the black boxes be extremely limited in the amount of data they collect and that the cars' owners be the only ones with access to it without court orders. Given the history of this sort of surveillance, though, there's plenty of reason to believe that the use of the black boxes will grow and its role expanded.

Once this technology is connected and linked to police, we can expect it to be used to remotely disable vehicles when police want. We can also envision it being used to limit a car's ability to drive faster than the speed limit, because the car's black box will "know" where it is. Your driving experience is about to get a lot more controlled

because of this technology—and you're not going to be able to hide anything you do while you drive.

Monitoring Political Speech

In 2006, the U.S. Department of Homeland Security issued a "protective intelligence bulletin" from the intelligence branch of its Threat Management Division. The bulletin contained a calendar that provided details about more than 70 peaceful political advocacy groups.

There wasn't any reason to think that any of these events were going to be anything other than peaceful. It was just an example of the Federal government's desire today to track and monitor any political speech that falls outside of the narrow bounds of what is considered acceptable by the political mainstream. The message from the government is simple: If you don't agree with everyone else, you're a potential enemy.

Although the ACLU filed a complaint with the DHS, the organization concluded—three years later—that it has the right to monitor political organizations as it saw fit, but the agency said the memo justifying this legal position was classified and couldn't be released.

The government's extreme distrust of anyone with opinions that diverge from the majority became even more plain in 2009 when a DHS-affiliated center in Missouri released a report called "The Modern Militia Movement." The document was intended to give Missouri law enforcement agencies guidelines about the warning signs to watch for in potential domestic terrorists.

What did the government consider to be the sign of a potential terrorist? The document said to be on the lookout for political bumper stickers for third-party Presidential

candidates such as Ron Paul. (Although Paul once ran as a Libertarian Party candidate, he's run as a Republican for years, including in the year before the report was written.) In addition, it was supposed to be a "red flag" if citizens talk of conspiracy theories or possess "subversive" literature. This stunning document leaves the impression that pretty much anyone who opposes the government is a potential terrorist. It's chilling to read.

But this document was just an echo of a DHS document titled "Rightwing Extremism: Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment," that named as potential terrorists "disgruntled" military veterans returning from Middle East battlefields, people who fear declarations of martial law and suspension of the U.S. Constitution, those who stockpile food, ammunition and weapons, those opposed to illegal immigration, those who oppose gun control laws and people who "bemoan the decline of U.S. stature and have recently focused on themes such as the loss of U.S. manufacturing capability to China and India."[4]

In late 2011, the Department of Homeland Security was forced to admit in court that the agency has contracted with General Dynamics to monitor online speech. The contract requires the company to identify "media reports that reflect adversely on the U.S. government, DHS, or prevent, protect, respond government activities." The contract also requires General Dynamics to generate reports on what is being said online about "DHS, Component, and other Federal Agencies: positive and negative reports on FEMA, CIA, CBP, ICE, etc. as well as organizations outside the DHS."

In other words, the government you're paying for is taking your tax money and spending it on finding out whether

anyone is saying anything critical about that government.

Are you worried about your privacy yet? You should be. But there are some things you can do to maintain some semblance of privacy without actually dropping completely off the grid.

Safer Surfing

Reading about the ways government and corporations are watching what you're doing and how thieves can steal your information through your computer may give you pause about using a computer at all. But don't let the danger frighten you away from the computer altogether. The Internet is still a great source of information, an excellent way to research, locate and buy products not easily found in the local mall and an excellent way to keep in touch with friends and family around the globe. You just have to use a little common sense—and take advantage of some readily-available technology—in order to ensure you're using the Internet safely.

And one of the basic common-sense rules is to always use a virus protection program when using the Internet. This is a program that checks your computer to make sure a virus or Trojan file or program hasn't been downloaded—whether inadvertently or not—onto your computer. Viruses can enable others to get into your computer information or destroy your files. There are several that you can use for free—try AVG, available at *http://free.grisoft.com/freeweb.php/doc/1/*—or you can choose to pay for protection from a company like McAfee or Symantec.

Be sure you keep your programs updated. Programs that need to be patched are weak spots through which intruders can more easily gain access to your computer.

To protect yourself you need to keep all of the software you've purchased patched with all of the patches provided as updates by the vendors who write that software. Each vendor will tell you where to find and how to patch and update the software you've purchased.

Use care when reading email with attachments. Email attachments that you weren't expecting are often viruses. Your virus software, if it is up to date, should catch and quarantine any virus, but it is best not to take a chance.

You should never click on links that come in your email. Many of them are phishing efforts. First, find out where the link is actually pointing (put your mouse over but do not click the link: if the address is suspicious, pointing to a website in Russia for example, then you know it's a fake.) Clicking on it in your email program opens the door for a virus to get inside your computer.

Be suspicious of any emails you receive that are ostensibly from your bank or financial institution. If you have a "warning" from your bank, then go to your bank directly in your browser, log on, and see if the purported message is there. If it isn't, then the one in your email is not real. But you should also know the bank's policy about notices. It's highly unlikely the bank would approach you that way if there's a problem with your account.

Install and use a good firewall program to block outside attempts to gain access to your computer. A firewall program works like your locked front door that keeps unwanted people out and your toddler in. If intruders can't get to your computer resources, they can't use them for their purposes.

If you want to advance to the next step in computer privacy you can install a program that allows you to browse completely anonymously. When you contract with an

Internet service provider (ISP) for Internet access, the ISP assigns an IP address to your computer when you log on. The address looks something like this, with the "x" symbols representing numbers: xx.xxx.xxx.xx. In an ideal world, that ISP would be randomly assigned each time you log on. But in our post-9/11 world, and through efforts to stop file sharing over the Internet, things today are far from ideal. So most ISPs have yielded to government and corporate pressure to assign an IP address that remains with each computer for months at a time, and that IP is tied to your billing address.

The IP address is visible to anyone who has access to the back (technical) end of a website. This can give snoops—government and otherwise—an open gate to stroll through into your personal life.

For example, perhaps you have used file-sharing sites to share songs or movies. If the movie or recording industries—which hold great sway over Congress through their lobbying activities—decide that file sharing is a copyright violation (as they did a few years with Napster) they can file suit and get the courts to require the ISPs to divulge the names and addresses of the file traders. The movie and recording industries can then use the threat of an expensive lawsuit against individuals to extort money from the traders (or their parents if the file sharers were minors).

Or, say you've blogged something the government doesn't like. Law enforcement officers can get a warrant to acquire the customer information from the ISPs and learn who you are, where you live and what websites you've visited.

But catching "wrongdoers" using ISP information is not an exact science, as the Evansville, Ind., police learned in June 2012. Executing a search warrant for computer

equipment police believed was used to make anonymous threats against police officers and their families, police officers dressed in protective gear threw a stun grenade into a house, bashed in the door and stormed inside. They soon learned they had the wrong house. Apparently, the person making the threats had sat outside the home and used the family's unsecured Wi-Fi connection.[5] Of course, this is not the first time law enforcement has gotten it wrong, and it won't be the last.

The lessons here are two-fold: protect your IP and secure your Wi-Fi.

To protect your IP you should use an anonymous proxy site or a program that changes and hides your IP. The Tor Project produces software for different computer platforms that makes it appear as though your computer is somewhere else and that it's a different kind of computer entirely. You might be using a Macintosh to log in from Chicago, but



you could show up online as a Windows computer coming from somewhere in Italy. If you have reasons to avoid people knowing where you are, don't log into the Internet without using something like this. You can get the free software at *www.torproject.org,* although some people will need some technical help to set it up. There are other similar programs online that will accomplish this as well. A search using most search engines can provide you links and more information on these programs proxy sites.

If you have a home Wi-Fi network that you use to log onto the Internet with your laptops or gaming systems, you need to be sure to secure it. Most have a way to encrypt the network to at least limit, if not prohibit, unauthorized use. The website *PCworld.com* has a step-by-step description of how to do this at *http://www.pcworld.com/article/130330/how_to_secure_your_wireless_network.html.*

If you use wireless Internet at your home, take your computer outside and see how far from the home a signal is available. If it carries to the street, neighboring houses or a location that would allow someone to steal your signal, you should modify the signal to reduce its range. One way would be to create shields of dense material to line the walls and reduce the strength of the signal.[6]

Your web browser also stores information in the form of small bits of code called "cookies." Cookies can contain a variety of information, including your name, address, passwords and what sites you visit. Search engines like Google grab these cookies and use them to constantly plaster on the web pages you visit advertisements for products and services you have shown interest in through your browsing history. Always set your browser to delete cookies once it is closed.[7]

Use strong passwords to protect your information. These days, most computer access requires a login and a password. Selecting a strong password makes it harder for intruders to access your computer resources. Don't use numbers or letters in sequence, like 1234 or abcd, but use a combination of letters, numbers and symbols. Don't use names of relatives or pets. A hacker got into Paris Hilton's cell phone directory and accessed all her telephone contacts because the password was the name of her dog.

Hackers now have programs that run through common words and combinations and can crack the passwords used by most people in minutes, if not seconds. But using a long string of letters (both capital and small) interspersed with numbers and symbols will make a hacker's task more difficult.

There is also software available, called password safes, that can help you keep up with your passwords and keep them secure. This allows you to use more complicated passwords containing letters, numbers and symbols. Some are freeware and some must be purchased.

Use care when downloading and installing programs, especially from third party vendors. The Internet is a powerful resource for finding and using the work of others to enhance your computing resources. Programs are one example. Remember that not all programs on the Internet are what they say they are. Some programs contain or are viruses.

Install and use a file encryption program and access controls. Access controls are attributes of files and folders that limit access to only those who should have access. As a failsafe, encryption scrambles file contents so that only those who should have access to a file and know the decryption keys can see a file's contents.

Your passwords and other information can also be obtained by anyone who has access to your computer. There is hardware and software available that records your keystrokes. One company, SpectorSoft *(www.spectorsoft.com),* advertises its keystroke monitoring software saying, "Automatically record everything your spouse, children and employees do online." The software is available for about $100. A free plug-in for your web browser called KeyScrambler Personal protects everything you type from keyloggers by encrypting your keystrokes at the keyboard driver level, deep within the operating system.

A piece of hardware called KeyKatch is a small device that can be attached to the back of your computer that can also record keystrokes—up to the last 64,000 for the most expensive model. It resembles a connector and while a person diligently checking for such devices behind the desktop computer will probably spot it right away, a casual glance by the untrained or unsuspecting will miss it.

These—and similar products—require someone to have access to your computer to install them. You can prevent unwanted programs from being installed on your computer by using a BIOS password to restrict unauthorized access. BIOS is the acronym for "basic input-output system." It is information stored in a chip in the computer that tells the computer what to do upon startup. A BIOS password prevents the computer from accessing that information and performing its startup routine.

Setting up a BIOS password requires a little technical skill, but instructions are available online. But be aware, a BIOS password can also be overcome with a little effort. But it will discourage most unauthorized use of the work station.[8]

It doesn't matter whether an intruder tries to gain access by sending you a virus as an email attachment, exploiting a program that hasn't yet been patched, accessing your system in a way that a firewall would normally prevent or installing something on your computer that allows monitoring. They're all examples of the same fundamental concept: Someone is trying to access your computer resources and you don't want them to have that access.

A good source of information on computer security measures, in addition to the bibliography at the end of this book is *www.cert.org.* Go there for more information.

And one more reminder: If you have something stored on a disk, whether it is the hard drive or a removable storage device, don't think that you can erase the data and remove it completely. There are many ways to retrieve information that you thought had long ago been deleted.

There is software available—some of it freeware—that does a competent job of removing data. Called wiper, wiping



or shredder programs, this software basically records new data over the old that you want removed. A little time and a search engine will help you locate them. These things come and go because there's not a big market for them, plus the government pressures programmers to either discourage them from writing such software or to cajole them into making it possible for investigators to see what has been wiped. Some good programs that may still be available are:

- DWIPER (freeware), *www.dpaehl.de*
- Mutilate File Wiper (shareware), *www.mutilatefilewiper.com*
- BCWipe (shareware), *www.jetico.com*
- Eraser (freeware), *www.heidi.ie/eraser/*[9]

While these are thought to be completely effective the bottom line is, if you have something on your computer that you absolutely don't want found, you have to completely destroy the hard drive or storage device that contains the information.

If you use an iPhone or iPad, Apple's iCloud system will wipe your devices on command. This is especially helpful if your phone or pad is lost or stolen. As long as the device has battery power, all you have to do is log into iCloud and tell it to wipe the device. It instantly becomes as clean as it was when it left the factory.

Keeping Your Emails Private

You can encrypt your email and make it more secure. Even though an encryption code can be cracked, most of today's encryption software makes it so difficult and time-consuming to do that it is not a worthwhile endeavor. One of the most widely-used email encryption programs is Pretty

Good Privacy (PGP). First introduced in 1991 by a programmer named Phil Zimmerman, the software was so successful that the U.S. government went after it tooth and nail. Zimmerman was harassed by the Bill Clinton Administration with a three-year criminal investigation and attempts to quash its release by classifying it as a munition. The software eventually made it to the Internet and has been upgraded and refined ever since.[10] The freeware version is available at *www.pgpi.com*. The commercial version is available at *www.pgp.com.*

There are other ways to keep your emails private as well. One is to use an email provider that promises to keep your information private and is backed by a government that has demonstrated a history of protecting people's privacy. Swissmail is an email provider much like Gmail, Yahoo or AOL, but much different. When Swissmail promises to protect your privacy you can take it to the bank, just like you can Switzerland's private banking laws. Swissmail costs $35 per year for its services. It is easy to set up, can be accessed anywhere in the world, automatically encrypts all email transfers so they can't be read "in transit," and works seamlessly with email management programs like Microsoft Outlook.

But unlike Google, which routinely hands all of its email data over to the U.S. government agencies, Swissmail is private. And it is against Swiss law for a company like Swissmail to release private information to anyone, including the U.S. government.

Other companies that do much the same thing are Centurion, Mute Mail and Securenym. Hushmail also provides this service to emails sent from your mobile device, and Kept Private provides an additional secure Instant Messaging (IM) Service.

More Safer Surfing Tips

Most web browsers now allow you to choose ultra-private settings that make it more difficult for websites to track your IP address and other personal information. Using Firefox with some extra plug-ins—such as Ghostery, BetterPrivacy and TrackMeNot—can eliminate a lot of the surveillance threats. These plug-ins stop the hundreds of trackers, web bugs, pixels and beacons placed on your browser by Google, Facebook and 600 other online networks.

We told you on page 15 how Google and the other well-known search engines track and record your computer information and web surfing habits, but there is a search engine that allows you to view websites anonymously. Called StartPage, its privacy policy as of July 5, 2012, says, "As of this week, StartPage will no longer record browser type and platform information (also known as the "user agent") of our users." It promises not to collect personal information, record your IP address or the type of browser or computer you're using. It also allows you an option to view by proxy, so those monitoring the website won't get your IP either. So, if you're curious what *WikiLeaks* is all about but don't like the idea of government snoops taking down all your information when you visit that site (which they do), you can check it out via StartPage in complete anonymity.

For secure mobile messaging, CasperTech and TopCrypto can encrypt your SMS texts and data streams and mobile voice messages. For Google Android phones, there is a service called Good. Many people believe the ultimate protection—military standard encryption for all mobile devices—is Gold Lock.

The FBI and DHS now routinely spy on Twitter users.

But you can enjoy private Instant Messaging (IM) with new services such as Gale (which uses high-level cryptography for private instant messaging), Psst (a simple, free, no-frills Instant Messaging software and Fire (for Mac users). Other services include Bit Wise, Crypto Heaven, Secure Shuttle and Sonork.

If you want to write about sensitive subjects and don't like hackers or government spies to know who you are, make sure you host your website overseas in countries with strong privacy protections—such as Germany, Spain and Canada. Zentek International provides offshore domain hosting services where you still own the domain name but the details registered on "WhoIs" only consist of very basic information. U.S.-based webhosts such as Bluehost.com also provide privacy cloaking for $9.95 a year. When someone searches WhoIs databases for information about who created your website, they find only information about Bluehost and not you.

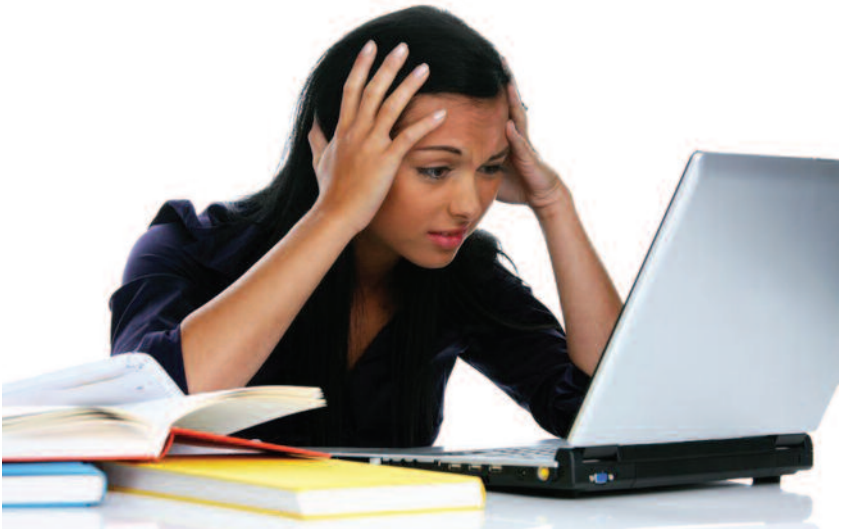
When you first sign onto a new computer or start up a newly installed computer program you are typically asked for personal information like your name, address and telephone number, at the very least. For greater privacy, simply don't use your real name! Many people type in "Computer User" in the space for computer user. The reason: Such information is easily accessible online whenever you visit a website. Simply not providing personal information in your hardware and software can greatly enhance your computer privacy.

Mozilla, the owner of the Firefox web browser, has an add-on that allows users to monitor in real-time how their actions are tracked and shared by various websites as they surf the net. Though currently experimental, the "Collusion"

add-on will allow users to turn off the tracking or record it anonymously for use by researchers, journalists and others to analyze how data is tracked on the web.

Don't want people to view your web browsing history? Just deleting via the options menu doesn't make it disappear. But using Free Internet Window Washer 3.1 will wipe a wide range of histories for Windows, Microsoft Office, Instant Messengers, Outlook Express, most browsers and long list of applications. It can be set to wipe these histories on demand, automatically upon startup or every few minutes. It overwrites the files you specify, which makes it impossible for even the best-equipped snoops to know what you've been up to.

Need to control what your employees—or even your kids or spouse—are doing on the Internet? Look at OpenDNS. DNS stands for Domain Name System, and according to *Wikipedia* it is a hierarchical naming system for computers, services or any resource participating on the Internet. One of the things it does is translate humanly meaningful domain



names to the numerical (binary) identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide. In simpler terms, it serves as a virtual "phone book" by translating computer host names into IP addresses (*www.example.com* becomes 200.73.622.182). OpenDNS uses this method and stops your employees—and kids, etc.—from going to gambling or pornography sites. It also spots and flags "phishing" sites. And best of all, it's a free service.[11]

Keeping your computer free of any incriminating data is your best defense, should some law enforcement agency decide to issue a subpoena to get their hands on it. You should destroy all old emails that are stored on your computer. The data you store on your computer should be encrypted. Always use secure passwords. And remember, you're under no obligation to reveal your passwords if asked.

CHAPTER 3

Banking in Secret in the Post-9/11 Era

The Federal government has created a massive databank filled with information about tax returns, bank accounts and even credit card purchases. FinCEN (Financial Crimes Enforcement Network, a branch of the Treasury Department) is the government's enormous financial data collection arm.

FinCEN operates by systematically collating and cross-analyzing law enforcement, intelligence, public and financial databases. It may have access to anything, from old IRS forms to your latest credit rating. FinCEN pulls in personnel and information from the IRS, FBI, DEA, Secret Service, as well as customs and the postal inspection agency. According to some experts, FinCEN taps into the National Security Council and the State Department's Bureau of Intelligence and Research.

FinCEN also gets information from bankers. If an operator at the FinCEN computer has just your name and a vague idea of where you live, or if you've left a "paper trail" in the form of a charge slip, he can enter the information into a computer terminal and quickly find your full name, Social Security number, date of birth, home address, driver license number and possibly bank account

numbers. If you have military service or criminal records, he can locate those, too, along with fingerprints or a photograph. Using the IRS database, the analyst can check on how much income you've reported and whether you've ever been audited or penalized by the IRS.

The USA PATRIOT Act and FinCEN

Financial institutions are scared to death of being fined or even shut down by the Federal government for being out of compliance with provisions of the USA PATRIOT Act. So, just to be safe, they are busily sending in information to FinCEN about their customers and filing reports on any customer activity the Feds may potentially regard as "unusual."

FinCEN reports show that banks are turning in their customers for investigation by FinCEN and the IRS for such "offenses" as making heavy use of an automated teller machine, for receiving or sending international wire transfers or because the bank does not know the source of deposited money. FinCEN requires securities investment advisors to create an anti-money laundering program as mandated under the USA PATRIOT Act. Firms must also appoint an anti-money laundering officer who will oversee the compliance process.

The USA PATRIOT Act also demands that firms adopt formal procedures for obtaining and inspecting client identification and for monitoring client transactions for suspicious activities. Failure to report suspicious activity to the government has resulted in fines and the permanent revocation of securities licenses. Under the Gramm-Lech-Bliley Act, the information kept on you by financial institutions and consultants must be protected. Information is not supposed to be given out without your authorization. However, the USA

PATRIOT Act essentially supersedes all other statutory privacy protections. Once the door is open to share information without your consent, there's no telling where the information may wind up. The information you share with brokers, financial planners, insurance agents, accountants and lawyers is highly sensitive—and highly prized.

Among the third parties who regularly try to access the records kept on clients are identity thieves, private investigators, marketers and government agencies. Have you received multiple letters from financial institutions proclaiming you are eligible for yet another pre-approved credit card? Chances are your financial history has been sold to the credit card company sending the letter. And who knows who else might have it?

This is just one of the intrusions you'll bear as a result of the sharing of your information. The consequences of having your private information "leaked" to unauthorized third parties can be ruinous, both financially and personally.

But the Gramm-Lech-Bliley Act has a provision that you can use to prevent your information from being shared with other bank entities or sold to third parties. Some time prior to July 2001 you received a notice in your statement giving you the option of preventing your bank or financial institution from selling your private financial information.

If you did not fill out that form and submit it then, it's not too late to do so. To "opt out," just send a letter to your bank or financial institution with the following information:

- Your name
- Your address
- Your account number.

Then, draft a letter stating:

Dear Sir or Madam:

I am submitting the following instruction with regard to my account(s) and your information sharing and sales policies:

In accordance with the provisions of the Financial Services Modernization Act (Gramm-Leach-Bliley Act) allowing me to opt out of any sharing or sales of my personal information, I direct you not to share any of my personally identifiable information with nonaffiliated third-party companies or individuals. I further direct you not to share nonpublic personal information about me with affiliated companies or individuals.

In accordance with the Fair Credit Reporting Act, which allows me to opt out of the sharing of information about my creditworthiness, I direct you not to share such information with any affiliate of your company.

I do not wish to receive marketing offers from you or your affiliates. Please immediately remove my name from all marketing lists and databases. I request that you acknowledge receipt of these instructions and your intention to comply with my request for privacy of my personal, financial and other information.

Thank you for your assistance in this matter and for taking steps to protect the privacy of your customers.

Sign and date your letter and mail or deliver it to your financial institution. The company is required by law to comply with your request.[12]

It is also a simple process to prohibit anyone from using information contained in your credit report from being used in any transaction not initiated by you. This will not only protect your privacy, but will also stem the flow of junk mail

to your mailbox by opting you out of credit report screenings by financial organizations. Call the automated opt-out number of the major credit reporting agencies (Experian, Equifax and Trans Union) at 1-888-567-8688. You will be asked for certain identifying information that will be used to exclude you from screening for pre-approved credit offers.[13]

Suspicious Activity Reports

A key weapon in the war on financial privacy is the requirement that financial institutions file a Federal Suspicious Activity Report (SAR) on anyone who engages in any "suspicious transaction relevant to a possible violation of law or regulation." According to the Treasury Department, "All financial institutions operating in the United States, including insured banks, savings associations, savings association service corporations, credit unions, bank holding companies, non-bank subsidiaries of bank holding companies, Edge and Agreement corporations, and U.S. branches and agencies of foreign banks, are required to make this report following the discovery of:

> Insider abuse involving any amount, violations aggregating $5,000 or more where a suspect can be identified, violations aggregating $25,000 or more regardless of a potential suspect, or transactions aggregating $5,000 or more that involve potential money laundering or violations of the Bank Secrecy Act."

The government began mandating SARs in 1992. The USA PATRIOT Act broadened the scope of SARs. Section 358 of the Act allows for the Central Intelligence Agency to receive these financial reports on citizens. The CIA is definitely back in the business of spying on Americans and is, with the help of SARs, creating files on perhaps hundreds

of thousands of citizens.

Almost any institution that borrows, loans or otherwise deals with money has everything to lose and almost nothing to gain by being uncooperative with the government. So they dutifully fill out the Suspicious Activity Reports and send them off to be filed away in FinCEN. With things as they stand, the push is for anything even remotely abnormal to get reported, since doing so takes the bank off the hook with regulators as well as the CIA, IRS, FBI and other government agencies that could cause the bank great harm. The law compels banks to report any transactions that have no "apparent lawful purpose or are not the sort in which the particular customer would normally be expected to engage."

This, of course, is an entirely subjective judgment, and banks are apt to err on the side of caution (which means that they can be expected to report anything and everything that seems the slightest bit out of the ordinary). FinCEN has the ability to identify and punish businesses that turn in SARs at a substantially lessened rate than the national average. To keep regulators off their backs, banks are "ratting out" a record number of unsuspecting customers to the Treasury Department.

Under the USA PATRIOT Act, when a financial institution files a SAR on a person, it is illegal for the "subject" to be told that a report is being forwarded to the government for analysis. Thousands of accounts have been frozen and perhaps millions of transactions have been cancelled by banks trying to comply with the USA PATRIOT Act.

Almost invariably, these "security" measures are carried out for no good reason. For example, in fall 2005, Wachovia Bank, apparently motivated by concerns over USA PATRIOT Act requirements, froze a "suspicious" bank account. The

account was used by nuns at Florida's Holy Name Monastery, who were not buying gifts for al-Qaida or doing anything else illegal with their account. The bank later apologized and reimbursed the nuns for hundreds of dollars in bounced check fees.

Currency Transaction Reports

Various financial institutions are also busily filling out secret "Currency Transaction Report" (CTR) forms on customers who engage in transactions involving $10,000 or more. And those suspect individuals who have several such reports filed on them may be audited by the IRS or investigated for dealing drugs. There are a lot of honest citizens who have their names attached to CTR forms, given that the banking industry is filing over 12 million CTRs each year. This government mandate also prevents banking officials from revealing to customers their compliance with the CTR system. Telling you could mean a 10-year jail sentence or a $500,000 fine per offense.



If you ask about what information may be reported to the Feds, bank employees either have to lie or beg ignorance. Those who know about this law can structure their withdrawals to avoid hitting the $10,000 limit. But such "structuring" is also illegal. If you appear to have planned withdrawals to avoid hitting $10,000 at any given time, bank employees are instructed to file a special form that suggests you might be trying to circumvent the law. So be careful when withdrawing more than (or close to) $10,000 in cash from a bank account. Doing so may jeopardize your financial privacy and security.

With all this talk of government-authorized bugs, wiretaps and financial investigations, you might be thinking, "For the love of Pete, is anything sacred anymore?" Definitely not the mail processed by the U.S. Postal Service—which does its fair share of snooping into the letters and packages you send and receive.

Avoiding the "Eagle's Eye"

Since the government has been able to force banks to adopt policies that encourage them to turn over private information about customers, it isn't surprising that a government agency like the U.S. Postal Service would have a customer-snooping program of its own. Working under the "Eagle's Eye" program, the Postal Service has managed to transform the symbol of our Nation into a bird that preys on citizens' privacy.

This program, reported on the floor of the U.S. House of Representatives by Representative Ron Paul (R-Texas) in June 2001, was initiated in 1997. It teaches Postal clerks to report nearly anything more "unusual" than a stamp purchase. Eagle's Eye also applies to money orders issued by the Post

Office. Under USC 31 Secs. 5313(a) and 5324, Postal employees must report, on the same day, money order transactions between $3,000 and $10,000, as well as any apparent "structuring" of transactions to avoid reporting requirements. Post Office employees are instructed to avoid telling customers about this law (with some anti-crime bills suggesting that telling a customer makes the postal clerk a "co-conspirator" in the crime).

It is a crime, under U.S. Treasury Department regulations, to mail "excessive" amounts of money to other countries. What many people fail to notice is that this same regulation applies to actions that "cause" $10,000 to be shipped or received, including not only cash shipments, but "other monetary instruments." In fact, when all the fine print is read, any action involving $10,000 (actual cash or wired money or a check), will sound the alarm bells with a clerk compelled to fill out a "Report of International Transportation of Currency or Monetary Instruments" form to report the "suspect" engaged in such an act.

Those receiving money or money orders can be forced to forfeit their payment if government officials suspect the sender might have used the mail at any point in the commission of a crime (with drug dealing being the general charge). The money often remains in the hands of government agencies—even if no charges are ever brought against the individual it was confiscated from.

It's illegal for a government employee or any other unauthorized person to open your mail, but government agents have a number of ways of getting inside your mail "legally." The FBI has a number of tools to get the job done without even breaking the seal. Special lights,

chemical sprays and ultra-sensitive x-ray machines can often reveal the contents of a piece of mail.

Here are some tips for protecting your privacy when you need to mail or receive letters or packages and tips for avoiding the Eagle's Eye at the Post Office:

- Avoid purchasing money orders of $500 or more at the Post Office.
- Never get a post office box. (I explain how to receive mail privately on page 134.)
- Use private carriers like UPS and Federal Express for mailing valuables and important documents. (However, you shouldn't assume that packages handled by private carriers are beyond the government's reach. Government agents may inspect any UPS or FedEx package that seems "suspicious." Private carriers generally will completely discard their privacy and security policies in order to satisfy government agents.)



- Double wrap your envelopes. Use a clear packing tape to completely enclose the envelope covering the entire paper surface with the tape. Then put this into another envelope. If the inner envelope is tampered with there will be ample evidence to reveal it. This also makes the contents impervious to chemical sprays that private investigators or other snoops might use to peer inside. The packing tape makes it impenetrable to the spray.

Federal Snooping Via "Data Mining"

Government snoops engage in data mining by analyzing credit card purchase records and other private-sector financial transactions made by individuals. Data mining came to public attention in the wake of adverse publicity over the Pentagon's "Total Information Awareness" project, which involves the use of Pentagon computers to track many aspects of citizens' buying and travel habits.

Shortly after the Pentagon's Total Information Awareness spy program was unleashed in 2002, it was shut down due to public backlash over its audacious scope. *The National Journal* has reported that Total Information Awareness "was stopped in name only." The overriding mentality of our nation's intelligence agencies remains that of a giant eye gazing out over the entire globe, entitled to know everything about anyone. A little-known system called Analysis, Dissemination, Visualization, Insight and Semantic Enhancement (ADVISE) is now assuming a large role in the government's data mining efforts. According to the *Christian Science Monitor* (Feb. 9, 2006), "Only a few public documents mention it." Even most Congressman don't know it by name and certainly don't know the extent of ADVISE's activities.

Documents obtained under the Freedom of Information Act by the Electronic Privacy Information Center (EPIC) confirm that in addition to the Pentagon's data mining programs, many Federal law enforcement agencies have quietly set up data-mining operations of their own. One private software firm, Visual Analytics, for example, already tracks some people who use ATM banking cards and make phone calls (tracking is done on behalf of clients, the National Security Agency and the Defense Intelligence Agency).

The IRS believes it has a lot to gain from data mining—namely, more of our money. Sifting through private business records will be much easier for the IRS once all business documents are in electronic form. All these new filing requirements will give the IRS plenty of information to decide who'll be targeted for tax audits! Here's what you need to know to keep YOUR name off the list.

Avoid Throwing Up Audit Flags

According to a Jan. 6, 2012 article on *CNNMoney.com*, the IRS audited one out of every eight millionaires in 2011, the third year in a row the agency increased its surveillance of the nation's top earners. About 12.5 percent of all taxpayers earning $1 million or more were dealt audits in 2011, up from 8.4 percent in 2010 and 6.4 percent in 2009. But lower earning taxpayers were also scrutinized more heavily as well. In 2011, one in 25 of those earning less than $200,000 per year were audited compared to one in 32 in 2010.

The IRS was also on the lookout for people who had their money stashed in offshore accounts, many of whom were wealthier taxpayers, IRS spokeswoman Michelle Eldridge told *CNNMoney.com.*

High on the IRS's hit-list are self-employed business

people, independent contractors, partners, S corporation shareholders, gamblers and employees who receive tips. According to the IRS website, a variety of methods are employed to select which returns are audited:

- **Potential participants in abusive tax avoidance transactions:** Some returns are selected based on information obtained by the IRS through efforts to identify promoters and participants of abusive tax avoidance transactions. Examples include information received from "John Doe" summonses issued to credit card companies and businesses and participant lists from promoters ordered by the courts to be turned over to the IRS.
- **Computer scoring:** Some returns are selected for examination on the basis of computer scoring. Computer programs give each return numeric "scores." The Discriminant Function System (DIF) score rates the potential for change, based on past IRS experience with similar returns. The Unreported Income DIF (UIDIF) score rates the return for the potential of unreported income. IRS personnel screen the highest-scoring returns, selecting some for audit and identifying the items on these returns that are most likely to need review.
- **Large corporations:** The IRS examines many large corporate returns annually.
- **Information matching:** Some returns are examined because payer reports, such as Forms W-2 from employers or Form 1099 interest statements from banks, do not match the income reported on the tax return.
- **Related examinations:** Returns may be selected for audit when they involve issues or transactions with other taxpayers, such as business partners or investors, whose returns were selected for examination.

Other: Area offices may identify returns for examination in connection with local compliance projects. These projects require higher level management approval and deal with areas such as local compliance initiatives, return preparers or specific market segments.

The IRS schedules audits a year in advance, so late-filed tax returns are actually given lower priority. Business owners who report only modest incomes combined with high deductions are a red flag. Dishonest or incompetent return preparers draw IRS attention.

In such instances, ALL clients of that preparer are at higher risk of audit. The same is true of shady tax shelters. Here are some tips to hopefully avoid closer scrutiny than normal:

- Steer clear of all but the most conservative and established tax shelters.
- Stay off the membership lists of "barter clubs." Some clubs cater to members who trade goods and services on a cashless basis. The IRS routinely forces clubs to turn over the names of their members.
- Never place deductions under "miscellaneous." If you can't categorize a deduction, the IRS may conclude your paperwork is sloppy.

Politicians and the liberal media frequently bemoan the so-called "tax gap," which supposedly represents the difference between amount of taxes owed the government and the actual amount collected. The truth is that most taxpayers overpay the government. They do so because they let the IRS withhold excess money from their paychecks, they are unaware of tax breaks that the law allows, and/or they choose not to take legitimate deductions for fear of throwing up red

flags that could trigger an IRS audit.

There are a lot of myths surrounding alleged audit triggers. You may have heard that you shouldn't claim this or that deduction because the IRS will audit you if you do. Chances are good that if your numbers raise no suspicions with IRS, you won't be among the roughly 1.5 percent of taxpayers who are audited every year.

Legitimate deductions rarely trigger an audit. However, IRS computers and bureaucrats do look for "red flags" that suggest (rightly or wrongly) that a taxpayer may be fudging or exaggerating or underreporting. Among the most common red flags are:

- Required forms are missing.
- Forms are not completely filled out.
- Forms are riddled with obvious errors or omissions.
- Reported income is less than that indicated by tax documents (W2 Forms, 1090 Forms, etc.).
- All figures are "round" numbers (i.e., "$5,000" instead of "$4,997"), implying the filer is just guessing or outright making up the figures.
- A waiter fails to report tips or reports them as an unusually small amount.
- An income in excess of $100,000 is reported (this factor alone more than doubles the likelihood of being subjected to an audit).
- Tax-protest literature or anti-IRS comments are included with a return (anyone who goes this route is begging to be audited; if you want to express your displeasure to the IRS for all it has done to erode your freedom, do so in a separate mailing—better yet, do so anonymously).

- Business losses are claimed to offset other forms of income.
- Itemized deductions appear to be arbitrary or phony. Itemized deductions are unusually high or low given the filer's reported income.
- Foreign asset holdings are reported.

As you can surmise, the single biggest audit trigger is inaccuracy. So don't try to alter or scale down your legitimate deductions just to make them appear more "normal." If you can back up each of your deductions, go ahead and take them.

Be Wary of Going Electronic

In 1998, Congress passed the IRS Restructuring and Reform Act—sweeping legislation that was supposed to change the way the government collects taxes. Many valuable new protections for taxpayers became law. Unfortunately, the bill also contained some highly questionable provisions.

At the core of IRS Restructuring was the push to establish a paperless return system in which all tax forms will be sent to the IRS electronically. However, convenient and efficient this may sound, it poses serious threats to privacy. IRS officials would ultimately like all financial transactions to be electronic so that they could be monitored and tabulated by IRS computers. Someday, the IRS could have enough information about you to simply prepare your return for you and send you a bill!

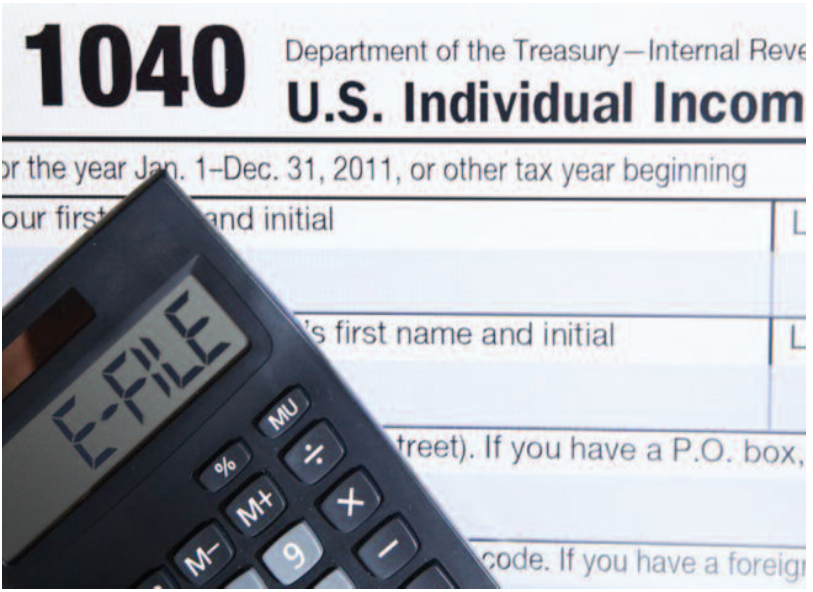
Beginning Jan. 1, 2012, that IRS provision became essentially a reality. On that date, any tax preparer who anticipates filing 11 or more tax returns a year was required

by the IRS to use the e-file system (unless a hardship waiver is acquired). The requirement was specific to tax preparers. Individual tax payers could still use a professional tax preparer and file a paper return or file a paper return if the individual himself prepares the return.

Should you consider filing electronically? Perhaps the one advantage to filing electronically is that your return cannot be lost by the Post Office or misplaced by IRS paper-pushers.

However, by using certified mail (or better yet, registered mail), you can get proof of when the IRS receives your return. With a certified mail return-receipt, you can avoid penalties the IRS may try to impose if it claims it never received your return.

Anytime you make the IRS's job of compiling data on you easier, you're making it easier for them to single you out for an audit or assess you for additional taxes or



penalize you. The IRS is now able to peruse data on individuals' financial activities kept by FinCEN or pry directly into the files kept on individuals by credit cards, banks and even casinos. Every time you swipe a card or sign a check, you're creating a permanent record of your activity.

The reality is that electronic filing is an enforcement tool for the IRS. To the extent that you can avoid making electronic financial transactions and avoid filing electronically, you'll make it a little bit harder for the IRS to gather and assemble information on you—information that could most definitely be used against you. Some government snooping is clearly aimed at grabbing as many of your hard-earned dollars as possible.

Identity Theft

Government and corporations aren't alone in using data mining. Identity thieves do it, too. The Federal Trade Commission estimates that as many as 9 million Americans have their identities stolen each year.

Anytime you are online there is someone, somewhere attempting to reach into your computer, locate your personal data and steal it so they can shop on your dime, or do something even more nefarious with your identity. Thieves then use the information to, among other things, take out loans, obtain credit cards, steal money from the victim's account, rent property, establish utilities or obtain a job. Often, by the time the theft is recognized a person's finances and credit are in shambles. And it's not just adults who have to worry. More and more identity thieves are targeting the identities of children. Identity thieves are even using the identities of the recently deceased because it takes longer

for the activity to be discovered.

And thieves don't need to have a computer to steal information. Following is a list of ways the FTC says thieves steal identities (with and without a computer):

- **Dumpster diving:** They rummage through trash looking for bills or other paper with your personal information on it.
- **Skimming:** They steal credit/debit card numbers by using a special storage device when processing your card.
- **Phishing:** They pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.
- **Changing your address:** They divert your billing statements to another location by completing a change of address form.
- **Old-Fashioned theft:** They steal wallets and purses; mail, including bank and credit card statements; preapproved credit offers; and new checks or tax information. They steal personnel records, or bribe employees who have access.
- **Pretexting:** They use false pretenses to obtain your personal information from financial institutions, telephone companies and other sources.

If you think your identity has been stolen, take these steps as recommended by the Federal Trade Commission:

1. **Contact the fraud departments of any one of the three major credit bureaus as listed below.**

   Place a fraud alert on your credit file. The fraud alert requests creditors to contact you before opening any new accounts or making any changes to your existing accounts. As soon as the credit bureau confirms your

fraud alert, the other two credit bureaus will be automatically notified to place fraud alerts, and all three credit reports will be sent to you free of charge.

Equifax—*www.equifax.com*

To order your report, call: 1-800-685-1111; or write to:
P.O. Box 740241
Atlanta, GA 30374-0241

To report fraud, call: 1-888-766-0008; or write to:
P.O. Box 740241
Atlanta, GA 30374-0241

Experian—*www.experian.com*

To order your report, call: 1-888-397-3742; or write to:
P.O. Box 2002
Allen, TX 75013

To report fraud, call: 1-888-397-3742; or write to:
475 Anton Blvd.
Costa Mesa, CA 92626

Trans Union—*www.transunion.com*

To order your report, call: 1-800-888-4213; or write to:
P.O. Box 105281
Atlanta, GA 30348-5281

To report fraud, call:1-800-680-7289; or write to:

Fraud Victim Assistance
Division, P.O. Box 6790
Fullerton, CA 92634

2. **Close the accounts that you know or believe have been tampered with or opened fraudulently.**
3. **File a police report.** Get a copy of the report to submit to your creditors and others that may require proof of the crime.

4. **File your complaint with the FTC**. The FTC maintains a database of identity theft cases used by law enforcement agencies for investigations.
5. **Visit *www.ftc.gov/idtheft.*** The information you enter there becomes part of a secure database that is used by law enforcement officials across the nation to help stop identity thieves. The site also has links to useful information from other Federal agencies and consumer organizations.

When you open new accounts, use new personal identification numbers (PINs) and passwords. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your Social Security number or your phone number, or a series of consecutive numbers.



If the identity thief has made charges or debits on your accounts, or has fraudulently opened accounts, ask the company for the forms to dispute those transactions:

- For charges and debits on existing accounts, ask the representative to send you the company's fraud dispute forms. If the company doesn't have special forms, use the sample letter (available at *www.ftc.gov*) to dispute the fraudulent charges or debits. In either case, write to the company at the address given for "billing inquiries," NOT the address for sending your payments.
- File a complaint with the Federal Trade Commission.

You should always completely destroy sensitive documents such as old credit reports, credit card statements, tax documents, etc. That means shredding them instead of simply tossing them into the trash can. When buying a shredder, opt for one with cross-cut capabilities. Traditional shredders that merely cut papers into a few vertical strips may still leave you vulnerable. A persistent thief could piece documents back together. Even two or three strips of paper taped together could reveal your bank account number, Social Security number and/or other information that could enable a low-life to steal your identity. A cross-cut shredder essentially turns every document into hundreds of tiny confetti-like squares of paper that are virtually impossible to piece back together.

Establish a telephone password on all your accounts—banking and otherwise. A telephone password is a series of numbers or one or two words that must be given before any personal information is discussed over the telephone. This is necessary because the person handling inquiries about your account has no way of verifying the caller is who he is representing to be. Telephone numbers, addresses and

Social Security numbers aren't sufficient for security because they can be stolen from a variety of sources. Most legitimate businesses have already established a telephone password system or would be happy to accommodate you with establishing one upon request. Once established, if you ever call that business and aren't asked for the password, it's time to raise a ruckus with management.[14]

Protect Your Money By Moving it Offshore

Most of us have a psychological fence at the water's edge. We can't think outside of the U.S. But in today's world, believe it or not, there is greater opportunity and security in going offshore. In fact, you may have considered strategies for offshore living, residency, second citizenship, investing, bank accounts, etc. Or you may be keenly interested in a tax and asset haven.

There are a lot of options, all fully legal, that will give you leverage and privacy that you don't now have in the United States. These strategies are for people who do their homework. They are not to be taken lightly.

Since passage of the USA PATRIOT Act, foreign bankers as well as foreign countries are careful about dealing with American citizens. They don't want to incur the wrath of the U.S. government. And make no mistake; there are members of the government—including your elected representatives in Congress—who believe you are cheating the government if you take your money offshore.

After Facebook co-founder Eduardo Saverin announced he would denounce his U.S. citizenship, Senators Chuck Schumer (D-N.Y.) and Bob Casey (D-Pa.) unveiled a bill called the Ex-PATRIOT—Expatration Prevention by Abolishing Tax-Related Incentives for Offshore Tennancy

Act at a Capitol Hill press conference.

The bill would re-impose taxes on expatriates even after they leave the United States and establish residence in other countries and bar individuals like Saverin from ever re-entering the U.S. again. The proposal would also impose a mandatory 30 percent tax on the capital gains of anybody who renounces their U.S. citizenship.[15]

As of summer 2012 this bill, S.3205, had not made it out of the Senate Committee on Finance, had only four co-sponsors—all Democrats—and its prospects for passage were bleak at best. But it does demonstrate how certain members of Congress consider your money as theirs.

Offshore banking is a big business worldwide. There are estimates that $2 trillion to $5 trillion from the U.S. stashed in nearly 40 offshore banking havens that impose no taxes, guarantee privacy and cater to nonresidents. One-third of the entire world's private wealth is stashed in Switzerland alone.

Offshore banks, unlike most U.S. banks, are stockbrokers. This means that one can invest in almost anything with a foreign bank account. The big advantages of a foreign bank account or annuity policy are privacy and asset protection from U.S. litigation. This puts funds out of reach of suit-happy U.S. lawyers and government snoops.

One of the best foreign "bank accounts" is the Swiss annuity—it's perfectly legal and not required to be reported on U.S. tax returns because it's an insurance policy.

Swiss annuities are essentially insurance policies. You invest your money with one of the country's premier rated insurance companies and are issued a policy contract. You receive interest plus dividends upon maturity. You can

choose your schedule of receiving your returns.

Swiss annuities have the following great features:

- They are exempt from the 35 percent Swiss withholding tax.
- They are insurance policies and therefore are not bound by Swiss bank secrecy laws, which have come under pressure and intimidation from the U.S. in its efforts to stifle efforts by Americans to move money offshore.
- As insurance policies, rather than bank or investment accounts, they are exempt from IRS regulations on reporting and taxation of offshore investments. There is no requirement to report insurance policies to the IRS.
- At $1.01 to $1.03 (at the time of this writing) the Swiss franc is now worth more than the U.S. dollar. People who bought Swiss annuities using the Swiss franc, when the Swiss franc was worth only 70 cents, have done quite well. They made interest plus excellent currency gains.

Using offshore trusts and bank accounts can be an excellent way for U.S. citizens to legally and securely protect their assets and themselves from lawsuits. Offshore trusts offer an individual a fair degree of personal confidentiality, privacy and asset protection from a business client—or even an ex-spouse. Remember, to maintain your privacy, don't sign any waiver to give foreign banks the authority to release information about you or your account.

Besides the Swiss annuity there other offshore insurance policies available for asset protection. A U.S. tax compliant life insurance policy issued by a carrier outside the U.S. offers additional benefits:

- **Increased asset protection.** No protection for life insurance proceeds exists under Federal laws. While many states have enacted laws that provide limited

protection for life insurance policies, coverage varies from significant to non-existent. In contrast, many offshore jurisdictions provide statutory asset protection for the death benefit and investments held by an insurance policy. And, as a practical matter, it is much more expensive for a creditor to bring a claim before a foreign court than a domestic court.

- **Access to global investments.** Offshore insurance policies provide tax-advantaged access to international asset managers and to offshore funds that are generally not accessible to U.S. investors.
- **Increased privacy.** Domestic assets, including life insurance policies, can easily be discovered by private investigators with access to any of the hundreds of "asset tracking" services now existing in the U.S. In contrast, assets held offshore are off the domestic "radar screen" and cannot easily be identified in a routine asset search. The confidentiality statutes of some offshore jurisdictions are an additional barrier against frivolous claims and investigations.
- **Not reportable as a "foreign bank account."** A life insurance policy purchased from a non-U.S. carrier is not considered a "foreign bank, security or other financial account." This means that there is no requirement to report the existence of, or the income derived, from an offshore insurance policy to any government authority. However, depending on what country you purchase an offshore insurance policy from, it may be necessary to make a onetime excise tax payment to the IRS amounting to 1 percent of the policy premium.
- **Currency diversification.** Life insurance policies are free to make investments in non-U.S. dollar assets that

may gain, in the event of future declines in the value of the U.S. dollar.

Other Means of Asset Protection

Life insurance is a big investment for a lot of people. But like all other assets, you should make it as invisible as you can, and that means putting it out of reach of the system. The system was created to impoverish the people. Be aware of this.

A warning here: Most life insurance agents recommend and insist on selling you whole life insurance. They can, and will, give you many "reasons" why you should buy whole life insurance, but they won't tell you their main reason. Their main reason is because all life insurance companies train agents to solicit whole life or universal whole life insurance sales.

The insurance companies pay commissions based on the amount of the policy premium. The agent makes a bigger commission on whole life insurance policies because the premium on this type of insurance is much higher than the premium on term insurance. Most Americans have been sold on whole life insurance. American insurance agents have done their job well.

Whole life insurance is a rip-off and a fraud in most cases. Life insurance companies have absolutely no risk for your premium above the cost of the insurance. Under most policies, when you die, the company keeps your cash value and only pays the beneficiary the death benefit. If you die, your cash value is not yours. The insurance company keeps the cash value.

Whole life insurance builds cash value and this cash value can be grabbed by the IRS, lawsuits and just about

anyone else with a claim while you are still alive.

But there is a way to put life insurance cash values out of the reach of creditors, lawsuits and the IRS. You can make your beneficiary the owner of your policy. The owner does not have to be the insured. However, when you transfer ownership, you relinquish all rights of your insurance policy.

Suppose your life changes and you decide that you no longer wish for your named beneficiary to be your beneficiary or owner. Then you can just stop payment on the policy. However, by doing this you will give up all your investment.

One other possibility is when you sign your policy over to your beneficiary as the owner of the policy, get him or her to sign the policy back over to you, but don't file the second assignment of ownership with the insurance company unless you later decide you want to. Keep this document in your possession in a safe place. If you later decide you want to reclaim control of your life insurance and cash value, simply file the ownership papers with the insurance company. You can change your beneficiary on the same form.

Make sure, from the very beginning, that the change of ownership form also allows you to change the beneficiary on the same form. This is very simple and you can secretly own and control your life insurance and cash values.

NEVER, NEVER make your beneficiary your estate! If you do as many lawyers advise, you are putting the proceeds of your life insurance into probate and these proceeds then become taxable.

Term Insurance

Term insurance policies, regardless of the variation, do not have cash value accumulations. Term insurance is

simply described as dying insurance. For many people it is the best kind of insurance, especially for young people. However, as one passes age 65, term insurance begins to get prohibitive in cost.

You can reduce the face amount, thereby reducing the cost, or the policy can be converted to whole life insurance without any health qualifications. Most life insurance should be term insurance, at least up to age 65.

It is preferable to buy level term insurance, meaning that the premium will not increase while the term insurance is in effect. Term insurance is the best way to get the lowest cost insurance available and, at the same time, not have to worry about asset grabbers. Term insurance has no cash value to steal, and they can't touch the death benefit.

Spousal Gift Trusts

A Spousal Gift Trust is a type of irrevocable trust that provides complete asset protection for your spouse and descendants, and removes the trust assets from your estate and the estates of your spouse and descendants for estate tax purposes. A Spousal Gift Trust is especially designed to receive lifetime annual exclusion gifts to your spouse which would otherwise go unused. This type of trust is very similar to a "bypass" trust (one that bypasses Federal estate tax) at death.

With a Spousal Gift Trust, you irrevocably transfer assets (typically up to $260,000, but no more than $1 million) to a trust of which your spouse is trustee (or co-trustee) and beneficiary. In addition, you can make lifetime gifts of $13,000 per year to your spouse in this trust. Your children and other descendants can also be beneficiaries during your spouse's lifetime, or they can be remainder beneficiaries after the

death of your spouse. You can also give your spouse the power to appoint, at death, the trust assets for your benefit during your lifetime if your spouse predeceases you.

Both spouses can create similar trusts for each other's benefit, and thereby obtain the asset protection and estate tax benefits, but the trusts cannot be identical in all respects.[16]

Modern technology is, in many ways, making our lives simpler. It's easier to gather information, easier to transact business and easier to communicate with others. But it's also easier for people to learn more about us than we want them to know. So in many ways the same technology is making our lives more complicated—particularly if you cherish your privacy.

You can no longer easily drop completely out of the mainstream and fly totally under the radar. But, if you are diligent, you can blunt any efforts by Big Brother government to know all that you do all of the time.

CHAPTER 4

How to Keep Your Home Private and Secure

Your home is where you should feel most secure. But where just 50 years ago there were many communities in which residents rarely felt the need to even lock their doors, today door locks are just a small part of the security measures needed to secure your home and privacy.

That's because criminals are becoming more desperate and more daring. Where once most thieves were burglars who primarily sought soft targets like homes in which the occupants were obviously gone for the day, now they are using much more aggressive methods of thievery, including home invasion robberies and carjackings.

In one such case, seven Oklahoma City teenagers invaded the home of Robert Jett, 78, and his wife Joan, 74, in July 2011. According to reports, Robert Jett opened his door to a stranger ringing his doorbell at 4 a.m. The young man on his stoop said he had been in a car wreck and needed to use the telephone. When Jett hesitated, the man pulled a gun and pushed Jett back into his home. Six more young men followed them inside and started asking where the Jetts kept their money.

Jett was kicked and beaten, and then he and wife were tied up while the seven invaders ransacked their house for the next half hour. The men finally left—carrying with them

the Jett's cash, checks and some papers—in the Jett's car.

The Jetts were lucky. They lived to tell the tale and suffered only some bruises and mental anguish. But some home invasion robberies are even more violent. In North Palm Beach, Fla., in May 2012, a man forced his way into Christopher Woods' house demanding money and guns. Woods was shot during the ordeal. Three months earlier, in a neighborhood nearby, a man wearing a ski mask broke into a house trailer and demanded cash and jewelry. The intruder pistol-whipped the owner and threatened to kill him and his female companion if they called police. The thief made off with $7. Beatings, shootings and rapes often accompany home invasions.

And more and more are becoming deadly. In a March 2012 incident in Tulsa, a teenager forced his way into the home of Bob and Nancy Strait. He beat the elderly couple and left in their car. Bob, 90, recovered from his injuries. But 85-year-old Nancy died the next day.

An Internet search for "deadly home invasion robberies" shows they happen with surprising regularity. In fact, experts say that home invasion robberies like these are on the rise. As many as one in five homes in the United States will experience a break-in or some type of home invasion.

While most attacks are made on women and the elderly, no demographic is immune. But the simple fact is, most of the home invasion attacks would not have occurred if the homeowners had taken steps ahead of time to secure their homes and had not let their guards down.

Making Your Home a Secure Fortress

Securing the home involves much more than selecting door and window locks and, perhaps, installing an alarm

Never Invite the Police Into Your Home

This may sound counterintuitive, but the police are not your friend. Therefore, you should never invite the police into your home unless they are there to investigate the burglary of your property.

Why? They may be on a snooping mission and anything they see they think is suspicious they're either going to interrogate you about or they're going straight to a judge to get a warrant.

Police are trained manipulators and liars. They don't hesitate to lie to you to get some snippet of information that will implicate you.

So if a law enforcement officer knocks on your door, never say, "Come in." Talk to him on your porch or stoop, and keep him outside. If he persists, remember you have the right to demand he produce a search warrant first. If he doesn't have one, don't be afraid to say "No."

system. Experts recommend that the first step to home security begins between the front door and the street with a barrier of some kind. Even a passive one is better than none.

If you have a yard, a decorative fence can work as a first line of defense to discourage unwanted visitors; be they solicitors, burglars looking for an easy target or robbers set to harm you. The fence could do nothing more than channel traffic onto a sidewalk or driveway that has a sensor to detect and notify you that someone's coming. That reduces the chance of surprise and gives you time to collect your wits and observe who is visiting you.

Even better is a fence with a locked gate and a dog

patrolling the grounds. A locked gate will at least slow down an intruder, and a menacing-looking dog will deter all but the most determined attackers and serve to warn you ahead of time that someone is on the stoop.

Your yard should be neatly trimmed with bushes kept small and potential hiding places kept to a minimum. It should be well-lit. The ideal situation is to install lights with motion-sensors, as most intruders value stealth and surprise but don't like being surprised themselves. A light suddenly switching on will cause most intruders to pause and reconsider.

But if you don't have a yard, a simple, locked gate on the porch will do much to slow down or discourage unwanted visitors.

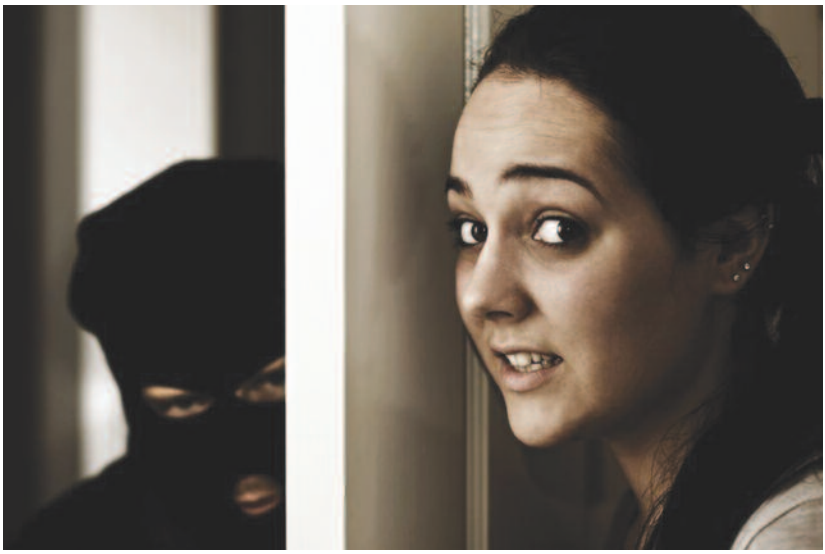
The next step is to make your doors more secure. It doesn't take Superman or a couple of police officers with a battering ram to break through most standard doors. While a good door will usually withstand a brute force entry attempt, a good swift kick or two is usually all that's needed to destroy the door frame and/or break out the lock setting. Privacy experts recommend installing steel-clad or solid wood doors—as opposed to hollow doors—and steel or hardwood frames for maximum security.

The door should fit closely in its frame and swing smoothly on strong hinges. The door should open inwardly to make defeating the hinges difficult to accomplish from the outside. If your door opens outwardly, make sure the pins can't be removed by welding them in place, installing a bracket that covers the pin, or by adding screws or bolts on the edge of the hinge-side of the door that recess into the frame and secure the door in place even when the pins are removed.[17]

While using a solid wood door increases your security, it decreases your ability to see who or what is going on outside. That's why a wide angle peephole is a must. It's crucial for you to have as wide a field of vision as possible so you can determine whether it's a good idea to open the door. Most of Robert Jett's attackers were hiding outside his field of view. It's a safe bet that had he seen seven men instead of one he wouldn't have even opened the door. And never depend on a door chain for security. It gives a false sense that it's safe to open the door to peer outside or communicate with someone as long as the chain is on. But that chain can be easily breached as it is held with only small screws.

When choosing a deadbolt lock, experts recommend getting one with the longest bolt available. This will require an intruder employing brute force to break through a larger section of steel or hard wood.

Covert entry teams usually have a skilled locksmith that can bypass most any lock he runs into. So for maximum



safety, a high-security "pickproof" lock should be installed. While there is technically no truly pickproof lock, there are some that are virtually pickproof under the conditions a sneak thief or covert operative would be facing in trying to gain entry to a home. Medco High Security locks are as close to pickproof as any.[18]

Lower windows panes should have the glass replaced with shatterproof plastic or reinforced glass. Burglar bars are another deterrent, but they can as easily lock you in as they lock others out.

And of course, a home security system is a must. It should have sensors that detect when doors and windows are opened in addition to motion sensors inside the house that detect movement.

To be effective, a home security system should do three things: sound a signal to warn of an emergency; cause fear and apprehension in any intruder, causing him to flee; and must serve as a call to arms, triggering a response to the emergency at hand.

The simplest route for installing a home security system is to contract with one of the large companies like ADT® and have them install and monitor the system. But companies can be required—or persuaded—by the government to assist them in defeating or disabling the system if government agents want to get into your home.

Another drawback is that when the alarm is tripped, precious minutes transpire before a police officer arrives at your home. While most burglars flee at the moment they hear the piercing sound of the alarm, some will continue with their lawless behavior knowing that they have a few minutes to work before police arrive. Today, thieves have little fear of telephone-based systems. Burglars know

they've got 45 seconds to 1.5 minutes to get in, get some goodies and get out before the police are called. They also know that the police get 98 false alarms for every actual burglary they are notified of by traditional security systems. So the average police response time is probably 15 minutes or more.[19]

Most monitoring companies will first call the home to determine if anyone is home and whether the alarm had been tripped accidentally. If the company fails to get an answer or the person answering is unable to provide the predetermined code, then the monitor will call police who, because of the number false alarm calls they receive daily, have other pressing matters to attend to or may be across town or across the county, may not arrive until the thieves are long gone.

Because of these shortcomings, a self-monitoring system may be a better choice than a centrally-monitored system like those provided by the big companies. A self-monitoring system can be designed to provide the first two necessary elements of an alarm system: sound the signal and cause fear and apprehension in the intruder. But a self-monitoring alarm system with an automatic dialer can be superior because it eliminates one of the steps involved in the process of determining whether the alarm has been tripped inadvertently or in response to an intruder.

The automatic dialer dials the homeowner and others the homeowner designates. The homeowner, knowing whether the alarm was tripped by accident or by an intruder, can then call the police himself. This creates a sense of urgency in the police department because the call is from a citizen as opposed to a monitor many miles away.[20]

Just remember, there are many ways an intruder can

gain access to your home. Here, courtesy of *The Prepared Ninja* blog, are 21 points to remember that you'll never hear from a burglar:

1. Of course I look familiar. I was here just last week cleaning your carpets, painting your shutters, or delivering your new refrigerator.
2. Hey, thanks for letting me use the bathroom when I was working in your yard last week. While I was in there, I unlatched the back window to make my return a little easier.
3. Love those flowers. That tells me you have taste… and taste means there are nice things inside. Those yard toys your kids leave out always make me wonder what type of gaming system they have.
4. Yes, I really do look for newspapers piled up on the driveway. And I might leave a pizza flyer in your front door to see how long it takes you to remove it.
5. If it snows while you're out of town, get a neighbor to create car and foot tracks into the house. Virgin drifts in the driveway are a dead giveaway.
6. If decorative glass is part of your front entrance, don't let your alarm company install the control pad where I can see if it's set. That makes it too easy.
7. A good security company alarms the window over the sink. And the windows on the second floor, which often access the master bedroom—and your jewelry. It's not a bad idea to put motion detectors up there too.
8. It's raining, you're fumbling with your umbrella, and you forget to lock your door—understandable. But understand this: I don't take a day off because of bad weather.

9. I always knock first. If you answer, I'll ask for directions somewhere or offer to clean your gutters. (Don't take me up on it.)
10. Do you really think I won't look in your sock drawer? I always check dresser drawers, the bedside table and the medicine cabinet.
11. Here's a helpful hint: I almost never go into kids' rooms.
12. You're right: I won't have enough time to break into that safe where you keep your valuables. But if it's not bolted down, I'll take it with me.
13. A loud TV or radio can be a better deterrent than the best alarm system. If you're reluctant to leave your TV on while you're out of town, you can buy a $35 device that works on a timer and simulates the flickering glow of a real television. (Find it at *www.faketv.com*)
14. Sometimes, I carry a clipboard. Sometimes, I dress like a lawn guy and carry a rake. I do my best to never, ever look like a crook.
15. The two things I hate most: loud dogs and nosy neighbors.
16. I'll break a window to get in, even if it makes a little noise. If your neighbor hears one loud sound, he'll stop what he's doing and wait to hear it again. If he doesn't hear it again, he'll just go back to what he was doing. It's human nature.
17. I'm not complaining, but why would you pay all that money for a fancy alarm system and leave your house without setting it?
18. I love looking in your windows. I'm looking for signs that you're home, and for flat screen TVs or gaming systems I'd like. I'll drive or walk through your

neighborhood at night, before you close the blinds, just to pick my targets.

19. Avoid announcing your vacation on your Facebook page. It's easier than you think to look up your address.
20. To you, leaving that window open just a crack during the day is a way to let in a little fresh air. To me, it's an invitation.
21. If you don't answer when I knock, I try the door. Occasionally, I hit the jackpot and walk right in.[21]

Thieves also watch the trash you set outside for signs of new electronics or other choice and valuable items that you have recently purchased. If you set the box outside that your new 48-inch HD TV came in, you're essentially taunting a burglar to step inside your home and take it. Boxes for expensive items should be burned or cut into small pieces and placed inside a trash bag.

Beware Telephone Eavesdroppers

Most people consider their landline telephones as a secure method of carrying on conversations. After all, party-line phones went away a long time ago. And law enforcement is required to obtain a warrant before it can tap your phone.

But convenience technology has opened a door to thieves that few consider. Cordless and cellular telephones provide thieves and government snoops an entryway into your private conversations.

Telephones are nothing more than radio transmitters. They send signals either from the cell phone to a cell tower, or in the case of cordless landline phones, from the handset to the receiver. If you are using an analog signal,

Smart Meters are Government Snooping Devices

The new "smart meters" being installed across the country ostensibly to reduce greenhouse gas emissions and lower utility bills are simply government devices designed to monitor your behavior and transmit it back to the utility company.

The goal is to have these meters installed in all homes as soon as possible. And as the Borg told Capt. Jean Luc Picard, "resistance is futile." One California resident learned this when he contacted his utility company to protest a smart meter's installation. He was told without the meter there would be no electrical service.

The meters are so sensitive at monitoring how and when electricity is used they have been used by law enforcement to detect people growing marijuana in their homes.

According to one electronics expert, the meters act as surveillance equipment by:

- Identifying individual electrical devices inside the home and recording when they are used.
- Monitoring household activity and occupancy.
- Transmitting wireless signals that can be intercepted by unauthorized and unknown parties.
- Collecting data about daily habits and activities which is stored in a central database.

In other words, by monitoring how you use electricity, government snoops are looking into every aspect of your life.

Source: *http://endoftheamericandream.com/archives/no-more-privacy-smart-meters-are-surveillance-devices-that-monitor-the-behavior-in-your-home-every-single-minute-of-every-single-day*

anyone with a receiver or scanner tuned to your frequency can listen in on anything you say.

Cellular telephones operate on 832 frequency pairs with 30 kilohertz (KHz) spacing in the 824.04 megahertz (MHz)-893.97 MHz range, and cordless telephones operate in the 43.72 MHz-49.99 MHz range, the 902.00 MHz-927.90 MHz range, and the 2.4 gigahertz (GHz) range. Any radio scanner can be programmed to receive cordless frequencies. New scanners have the cellular frequencies blocked, but anyone with proficient electronics knowledge can bypass the block.

Digital telephones are also radio transmitters and digital signals are unintelligible when heard on an analog receiver. But a digital receiver set to the correct frequency would allow the signal to be heard.

A technology called spread spectrum uses a broadband signal that is spread over a number frequencies and makes it more difficult to intercept and listen in on the conversation. It provides a clearer signal, yet prevents monitoring of the signal from those who aren't supposed to hear it.

Most of the latest cordless phones operate in the 2.4 GHz range, and only a few scanners are able to operate in that range. Purchasing a cordless phone for your landline that operates at 2.4 GHz will give you added protection from having your signal intercepted between the handset and base.[22]



Of course, none of these will protect you from phone taps. But there are relatively inexpensive devices available which will not only detect phone taps, but hidden

cameras, recording devices, GPS devices and more. Once such source is the Spy Exchange & Security Center in Austin, Texas, available online at *www.pimall.com/nais/countervideo.html.*

Voice Over Internet Protocol (VoIP) phone systems—which use an Internet connection rather than telephone cable, are typically less expensive than standard landlines and are much more secure. To use VoIP you need a high-speed Internet connection, a VoIP service plan and telephone equipment. Or you can go without the telephone equipment and, if you have a microphone for your computer, you can use free VoIP client software like Skype, or paid services like Iptel, Ekiga.net and ippi. Others include Cisco Telepresence, Facetime, Google Chat/Google Talk/Google Voice and OoVoo.[23]

Plus you can use VoIP with Secure Real-Time Transfer Protocol (SRTP) that has almost no effect on call quality; a unique encryption key is created for each call you make, thereby making eavesdropping extremely difficult for all but the most dedicated spies.[24]

You can also use your Skype account to make anonymous calls to telephones. You have to create an account in Skype and purchase the features, but once you've done so you can make your calls anonymously. You have to first set your preferences under the "call phones" tab to "deactivate caller ID." Skype has long been favored by those eager to communicate beyond the reach of government. Unfortunately the company has relaxed its privacy policy since its purchase by Microsoft and now gives authorities access to addresses and credit card numbers of its users.[25]

More calling tips:

- Always maintain an unlisted number. This will reduce

the chances of someone using readily-available public databases to find you.

- Use the caller ID, line blocking and call forwarding features provided by your carrier. These give you the advantage of screening your calls and blocking calls from someone trying to harass you.
- When calling someone, make your phone number appear as private. This provides privacy by hiding your number and creating the inability for them to call you back. You can do this temporarily each time you call by dialing *67. To set this feature permanently go to the phone's call settings menu and look for a setting called "Show/Hide My Number." (If this setting is not available, check the documentation that came with your phone or with the carrier's technical support team.) Select "hide number." Turn your phone off to save the settings, then turn it back on. Be sure you make a test call to check whether the change took.
- Use Google Voice to establish a telephone number you can give to people. You can set it to call your cell phone or landline and no one will know your true number(s).
- Use a spoofing service to disguise your number, change your voice, add background noises to your calls, send text messages that reveal a fake number or record your calls. These can be found using an Internet search engine.
- Use prepaid calling cards. You can buy these with cash and when you make a call from a landline the call shows up with the number assigned to the card rather than the number of the phone you're using.
- To protect your cell phone communications—both inside and outside the home—there are portable devices that create "white noise" while you talk that makes it

virtually impossible to eavesdrop on your conversation.[26]

- Remember that if you are like most people, your cell phone knows a lot about you. In many cases it contains passwords and other information you want to keep private. And all it takes is for someone to get their hands on your phone and they'll almost instantly be hacking into your accounts and/or stealing your identity.

Here are seven tips to help protect your cell phone's privacy:

1. **Beware of your phone's history of dialed numbers.** On all cell phones you have access to the list of recently dialed numbers and received calls. These numbers may contain information you typed on the keypad of your phone—information such as credit card numbers. It is important to clean up such information after making a private call. Keep in mind that not all cell phones record information at the same place.
2. **Keep contact list information simple.** Do you really need to keep your family member's addresses on your cell phone? If your cell phone is stolen, the thief will not only most likely learn who you are, but he will also learn who your family members are and where they live. Keeping your contact list simple and stripped of important information will definitively help protect your privacy.
3. **Remove important information from your agenda.** Most cell phones have a calendar feature which can also act as an electronic agenda. If you keep your appointments in there, a potential stalker will know about your next appointment if he can have a look at your phone. I'm not saying to forget the feature, but you might want to keep the information basic if you're concerned about your privacy.
4. **Erase sensitive text messages.** If you are using special

text message services like Paypal Mobile or even MSN Mobile, make sure you delete the history of sent and received messages containing information such as passwords or personal information.

5. **Disable the GPS feature.** Some cell phones have a GPS tracking feature, allowing for example automatic time change when you travel between time zones. This might be a little far-fetched, but if you are concerned about someone tracking you, you may want to turn off that feature. However, keep in mind that the GPS tracking feature can be important in the case of an emergency, as it allows 911 services to track you easier.
6. **Put a password on the cell phone.** Adding a password to your cell phone and locking it can help prevent information thieves from accessing your information. It will not stop a dedicated person from cracking the password, but it certainly will slow him down.
7. **Make sure you erase all personal information before you give the phone away.** If you want to give your cell phone away for recycling or sell it to another person, make sure you erase all information from the phone. Most cell phones have an option to erase all information and reset to factory default buried deep into their menu system.[27]

CHAPTER 5

How to Be Secure While Traveling

Police officers are trained manipulators. They take classes to learn how to read people's body language and how to ask open-ended and innocent-sounding questions in order to surreptitiously obtain information they can use against you.

They also have a knowledge of the laws that you don't possess—and laws differ from State to State, and even from one jurisdiction in a State to another. Police have also been known to invent "laws," place "evidence" that can be linked to you and twist your words into meaning something you did not intend.

For that reason you should never consent to a police search of your vehicle and never volunteer information when being questioned. Of course, not consenting doesn't mean you won't be subjected to an unConstitutional and illegal search, as Nancy Genovese learned.

Genovese was arrested in New York for taking pictures of a helicopter display outside the entrance to the Gabreski Airport in Suffolk County. Police confiscated her camera, searched her car without a warrant and then held her without charges. She then spent three days being interrogated, taunted, harangued, threatened, belittled, abused, humiliated, harassed and tortured by members of the Sheriff's Office. Then she was released, again without being charged. However, $5,000 was missing from her vehicle and her camera's

memory card was never returned to her.

You might think that she got what she deserved because she didn't cooperate, but two recent cases drive home the point of why it doesn't pay to cooperate with police: that of Army Lt. Augustine Kim and that of Diane Avera.

Before being deployed to Afghanistan, Kim left his gun collection with his parents in New Jersey. In the summer of 2010, Kim was back in the United States after being injured in a vehicle crash in Afghanistan. He had a medical appointment at Walter Reed Army Medical Center and decided to work a trip from his South Carolina home to his parent's New Jersey home around the medical center appointment.

He loaded his guns plus some spare parts in the trunk of his Honda Civic and headed to his medical appointment. He got lost in downtown Washington, D.C., and was pulled over by police. The officer said his license had been suspended, but Kim said he was not aware that it had been. It turns out the suspension was a clerical error caused by the State of North Carolina incorrectly reporting to South Carolina that Kim had failed to pay for a ticket.

But because of the erroneous suspension, the D.C. officer called for backup and told Kim he'd have to go to the police station. Then the officer asked if he could search his vehicle. Kim consented because he knew his guns were properly locked in a case, which complied with Federal firearms transportation laws. Kim was handcuffed and made to sit on the curb. He was then booked on four counts of carrying outside the home. Officers told him that he was in violation of registration laws because he admitted to having stopped at Walter Reed. In D.C., having a weapon outside the home is illegal.

In Demopolis, Ala., Avera answered a police officer's question honestly. It landed her in jail for 40 days—including 17 hours strapped in a restraint chair—and a conviction on a drug charge that carries a sentence of one year in jail and seven years of probation.

Avera had recently taken up the hobby of scuba diving. Her dive instructor had advised her to take pseudoephedrine (Sudafed®) to help her equalize pressure on her eardrums and to help her with other sinus issues she experienced while diving. This is a common practice among divers; and Avera had, under advice from her physician, taken pseudoephedrine many times before to treat allergies.

But just weeks before Avera was arrested, a new State ordinance went into effect in her home State of Mississippi that made pseudoephedrine a prescription drug. So Avera drove to Alabama to buy some.

In the car with Avera were her adult son, his girlfriend and their three children. The son and girlfriend bought two boxes of Sudafed® from a CVS. Avera bought another at Wal-Mart. As she pulled away from Wal-Mart, Demopolis Police Sgt. Tim Soronen pulled her over. (In Avera's trial it was revealed the CVS pharmacist was a police informant who tipped off police about the Sudafed® purchase.)

"What brings you to Demopolis?" Soronen asked.

"I came over to buy some Sudafed® for our scuba diving trip this weekend, since we can't buy it in Meridian anymore," Avera replied.

Soronen asked Avera if she knew it was against the law to cross the State line to buy Sudafed®. Avera said she did not. Soronen ordered her out of the car.

Using the threat of kidnapping Avera's grandchildren

and putting them into the hands of the State Department of Human Resources, Soronen extorted a confession from Avera that she was buying Sudafed® to manufacture crystal methamphetamine. It did not help that her son—a habitual drug user who had been through rehab several times—had a bottle of methadone and a pouch containing drug paraphernalia that police found during a vehicle search.

She was convicted after the trial judge allowed the prosecutor to make entirely unsubstantiated claims. These included that Avera had confessed to having used crystal meth for two years—her former employer, a physician, insisted there was never any indication she was a drug user—and that she had somehow "diluted" drug tests that showed she had no meth in her system.

Avera's conviction is being appealed, and she is free on a $20,000 bond. But Kim accepted a deal that allowed him to plead guilty of one misdemeanor charge of possessing an unregistered gun with the understanding the charges



would be dismissed and his guns and gun parts—worth $10,000—would be returned if he stayed out of trouble for nine months. Now the Metropolitan Police are refusing to release Kim's guns.

"The mistake he made was agreeing to a search of his vehicle," Kim's attorney Richard Gardiner told *The Washington Times.* "If the police ask for consent to search, the answer is 'no.' If they ask, 'why not?' The answer is, 'no.'"

For most people, encounters with police end with no more than a warning or a ticket. But you never know when you may say or do something that interests the officer enough that he or she wants to take a closer look at who you are and where you've been.

Privacy expert and lawyer Mark Nestmann writes in his book, *The Lifeboat Strategy* to never consent to a vehicle search. He reminds that you do not have to answer an officer's questions if you are being detained.

From his book:

> Say something like, "Officer, I know you want to do your job, but I can't consent to a search." A likely response will be, "Why not? What do you have to hide?" You are under no obligation to answer this question. Instead, say something like, "Officer, am I under arrest? If not, I would respectfully ask that you permit me to leave." If there's no response, then announce, "Officer, if you're not detaining me, may I leave?" If the response is "yes," say "thank you" and leave immediately. If the response is ambiguous, or if your question is answered by another question, repeat your question: "Am I being detained, or may I leave now?"

Avoiding Speed Traps And Traffic Cameras

Two electronic devices are essential for avoiding speed traps and helping to eliminate encounters with police: radar detectors and police scanners. Unfortunately, neither is foolproof.

A radar detector looks for signals in the frequency ranges in which police radar operates. When it detects a signal, it sounds an alert.

To be effective, the detector has to give you sufficient warning so you have time to slow down. But the police are deploying countermeasures that make detection as difficult as possible. Among these are flashing the radar only on cars they suspect as speeding, and "hiding" at the bottom of a hill and shooting cars as they come over the crest

By flashing individual cars, police keep the radar signal on for only a couple of seconds. The detector may sound, but driver may suspect it's just a false reading. The hill serves as a block and reduces the effectiveness of a radar detector.

That's why police scanners are also helpful. By monitoring police traffic you can learn of speed traps and driver license checks before you reach them.

To give yourself some protection from traffic light cameras, special license plate covers and spray-on coatings that defeat the radar cameras are available. These can be found by using an online search engine. Some companies that sell the covers or sprays include: OnTrack Automotive Accessories *(www.ontrackcorp.com),* PhotoBlocker Spray *(www.phantomplate.com)* and Veil *(www.laserveil.com).*

Source: Chesbro, *The Privacy Handbook,* pp. 217-218.

> If the response is "no," you're being detained. Police may detain you or your vehicle for a brief time… If you're detained, you're under no obligation to answer any questions or consent to a search. You should point that out; but again, in a non-threatening way. One way is to make a joke; e.g., "My lawyer would kill me if I consented to a search without him being present."… Specifically mention the word "lawyer." This will end many requests for a search or to answer questions. If not, tell the officer that you want to call your lawyer… If you don't have a lawyer… Just keep your mouth shut and don't consent to a search.

Nestmann also recommends you keep your car free from clutter and conceal everything that you want to keep private. If an officer sees something suspicious out in the open, he can get around the need for consent or a warrant and claim probable cause.[28]

If you are detained and searched, police can search your cell phone without a warrant, thanks to a ruling by 7th Circuit of the U.S. Court of Appeals. But while you're obligated to hand your phone over, you're not obligated to give cops the password to open up your phone. So always password-lock your phone and be careful what you keep on it. As a rule, today's smart phones carry a virtual cache of information about you. Once inside your phone, investigators can track down all your contacts, all your recent calls and all sorts of information you'd like to keep private.

Privacy experts recommend you keep one phone in your possession ready to turn over to police. It should have a few contacts—not necessarily real ones—and a short call and text message history. By giving it to police upon command you have satisfied, and possibly deflected, their desire to take

something from you they believe will be incriminating. Your regular phone should be secreted somewhere else in the vehicle—or better yet, left at home.

Privacy and the TSA

In this age of the DHS and its oppressive goon squad of perverts and pedophiles in the Transportation Security Administration, if you fly commercial—and sometimes if you use other forms of public transportation—you are automatically surrendering your 4th Amendment rights.

That's because you're going to be subject to either a public groping or an unhealthy dose of radiation just for the pleasure of being herded onto an uncomfortable airliner that may or may not get you to your destination on time. You can also expect your possessions to be scanned and your laptop, if you're traveling with one, to be searched as well.

It's essential, for privacy's sake, that you travel with a



wiped computer. You should save the important data you'll need in cloud storage. Cloud storage is a model of networked online storage where data is stored in virtualized pools of storage which are generally hosted by third parties.

Using an online email service like Yahoo or Gmail—or better yet, a secure service like Swissmail—is an example of using cloud storage. They store your email messages on their servers so those messages are not available to read from your computer without the proper login information (which you are under no obligation to provide to any law enforcement). The alternative is using an email program like Outlook or Mac Mail that stores messages on your computer.

When selecting a cloud storage provider, be sure you read the company's privacy policy carefully. If the company is eager to hand over your data to law enforcement or other interested parties, you need to find another.

CHAPTER 6

Maintaining Your Medical Privacy in an Obamacare World

The Patient Protection and Affordable Healthcare Act, also known as Obamacare, is sweeping legislation that when combined with a provision contained in the American Recovery and Reinvestment Act of 2009, make the biggest assault on medical privacy in our nation's history. While Obamacare drives everyone into a hyper-regulated health insurance system, the stimulus bill contained an amendment requiring the government to establish computerized medical records—called Electronic Health Records (EHRs)—that would follow each American from birth to death and forces physicians to participate or risk reduction in Medicare and Medicaid reimbursements.

The legislation creates a healthcare bureaucracy to handle the records under the oversight of a politically-appointed healthcare czar. The database will, at a minimum, include information on every American's race and ethnicity, according to a report on the technical media website *Cnet.com*. The information will be used for biosurveillance and public health purposes as well as medical and clinical research and will become part of a nationwide system for the electronic use and exchange of health information. More than 600,000 entities in government and business will have access to the

records.[29] It doesn't take a deep thinker to see a bureaucracy ripe for abuse.

After all, physicians know the most intimate details of our lives. As an example, consider this story told by Elizabeth Lee Vliet, M.D., on the website *News-medical.net:*

> It was a sad day recently when a married menopausal woman learned that her recent Pap test was positive for human papilloma virus (HPV). "How could this happen?" she asked. "I have not had relations with anyone but my husband since we married 30 years ago."
>
> Over the past year, her husband had several trips overseas for weeks at the time. She suspected the positive HPV indicated he had been unfaithful, but when she asked him, he said, "Oh, it can be latent for a long time."
>
> I showed her my records from 2008 and 2009: Paps were HPV negative. Her newly positive HPV likely means her husband had had sex with an infected person during his travels. She broke down weeping.
>
> HPV is an increasingly prevalent sexually transmitted disease that can hit women of all ages and increases the risk of invasive cervical cancer—another reason she was upset about becoming HPV positive. She now faced hard decisions. As she left, I felt sad watching her suffer with the impact of this news on her marriage.
>
> This kind of painful situation happens daily in doctors' offices. Such personal and private pain should remain between the patient, physician and family.

Under the new rules, this information will be open to view by insurers, government workers and a panel of government-appointed "experts" who gather to decide

what treatment is allowed for individuals based on certain criteria. But beyond that is the danger to the safety of your medical records. If hackers can penetrate even the highly secure Federal agency computers at the Pentagon and Department of Defense, how can you be sure your patient records aren't vulnerable? After all, hackers have already stolen millions of medical records from the Veterans Administration and those patients were placed at risk of identity theft.[30] And there are dishonest people all around you. Just ask Eric Drew.

While in the hospital receiving cancer treatment Drew had his personal information stolen by a hospital worker—and his life ruined. The worker got credit cards using Drew's information—and ran up debts. Despite proof that Drew had not opened those accounts, the banks and the credit reporting agencies refused to take the false information off his credit report, resulting in his inability to secure a mortgage.[31] And this occurred before potentially hundreds-of-thousands of people had access to his records.

According to a report on *Modernhealthcare.com,* records from the Department of Health and Human Services Office for Civil Rights show that more than 18 million individuals have had their patient records "breached" since September 2009.

And it's certainly not beyond the realm of possibility that those records could be used by law enforcement to open investigations against people who have not been accused of a crime. In 2010 the North Carolina Sheriffs' Association sought access to a State database of painkiller prescriptions that is currently only available to certain medical practitioners and was designed to alert doctors and pharmacists to possible "doctor shopping" by patients

in search of powerful painkillers like OxyContin and Percocet. The sheriffs' association argued their access would save lives by allowing them to arrest potential drug abusers. A report by the *Charlotte News & Observer* found that 30 percent of North Carolina residents had received at least one prescription for a drug on the list of controlled substances that appear in the database.[32]

It's possible that EHRs could be purloined to advance a political agenda or stifle a political rival of well-connected politicians. Presidents from Franklin Delano Roosevelt to Richard Nixon to Bill Clinton all had enemies lists and used personal information—in some cases, tax information taken from supposedly off-limits IRS records—against those enemies.

Those tax records are linked to a Social Security number. That means if you've given your Social Security number to your physician, your medical records are now linked to your tax records, making it easier for nefarious agents in government to learn your most intimate medical secrets.

Most physicians have, for years, been almost militant about the need to have your Social Security number on file. Hesitate to give it and the doctor's staff will look at you like you've suddenly sprouted wings. But the rule that would require you to provide physicians with your Social Security number was struck down by Congress before it was ever implemented. But that hasn't stopped most physicians' offices from asking for the information.

If they insist you provide them with the number, here is what you can do:

- Offer to pay cash for the service.
- Offer to provide a portion of your SSN—perhaps the

last four digits.

- Offer to provide another piece of identifying information such as a driver license or a document that has your blood type listed.
- Ask for the office manager and find out what their intent is for collecting the SSN. If they tell you they are required by some entity to collect it, ask what entity expects that. If they tell you it's the FTC or the Federal government, then tell them you know about the Red Flags Rule and that Congress struck it down.
- Understand that you may be at risk of being rejected as a patient if you simply refuse a doctor's office staff member who is adamant. In that case, you may be better off looking for a new doctor anyway.[33]

Ok, you may think medical privacy is no big deal. You have no political ambitions, so there is no danger of getting on the bad side of a powerful politician. But have you seriously thought about what your medical records contain and how they might be used?

Medical records are created when you receive treatment from a medical professional: be it a physician, nurse, dentist, chiropractor or psychiatrist. Records may include your medical history, details about your lifestyle (such as smoking or involvement in high-risk sports) and family medical history.

In addition, your medical records contain laboratory test results, medications prescribed and reports that indicate the results of operations and other medical procedures. Your records could also include the results of genetic testing used to predict your future health. And they might include information about your participation in research projects.

Information you provide on applications for disability, life or accidental insurance with private insurers or government programs can also become part of your medical file.

Financial records—your credit card, checking account and life insurance—may be there, especially information about where you go for medical coverage, how often you see the doctor and whether you have unpaid bills.

Employment information—particularly as it relates to Worker's Compensation claims, extended leaves, counseling (for mental illness, substance abuse, etc.) requested or ordered and whether you participate in any employer-sponsored health or weight loss plans—is certainly included.

Databases called IntelliScript and MedPoint report prescription drug purchase histories to insurance companies and will certainly be a part of your EHR. These go back as far as five years and detail drugs used, dosages and number of refills. By the way, you can request a copy of your MedPoint and IntelliScript reports. This is probably as crucial as obtaining regular credit reports (discussed on page 78) in maintaining your privacy and knowing what information may be in the public sphere.

To obtain your prescription drug reports:

IntelliScript—call 1-877-211-4816. You will have to provide your full name, date of birth, last four digits of your SSN and a current zip code.

MedPoint—call 1-888-206-0335

Or write: MedPoint Compliance, Ingenix, Inc.
2525 Lake Park Blvd
West Valley City, UT 84120

The Privacy Rights Clearinghouse *(www.privacyrights.org)* is a good source of information for learning more about

what the individual can do to protect his or her medical records. Following is a brief summary of the organization's suggestions for protecting your medical privacy:

- Discuss confidentiality concerns with your doctor. If you want a specific condition kept in confidence, present a written request to that effect. To be especially certain of confidentiality—especially from an employer paying for some or all of your health insurance—make an appointment with a different physician and use cash to pay for the visit.
- Ask the healthcare provider to use caution when photocopying your documents and insist that no more copies than necessary be made.
- Inquire about your healthcare provider's policy on the use of cellular and cordless phones and fax machines when discussing or transmitting medical information. Cellular and cordless devices are easy to eavesdrop on and fax machines are usually accessed by a number of people.
- If your records are subpoenaed in a legal proceeding, those documents become public records. But you can ask the court to seal those records.
- If your employer is self-insured, the human resources department probably has information about any health-related claims you've filed. You should discuss your privacy concerns with the administrator or department head.
- Before filling out any marketing surveys or questionnaires, consider what information you have to provide to receive free coupons or prizes.
- Before participating in health screenings hosted by shopping malls, hospitals or public entities, inquire

about how the information they obtain will be used. If you can't opt out of having your medical information shared with others, opt out of the screening.

- Use caution when visiting health-related websites and participating in online discussions. Remember what information you're revealing about yourself just by visiting the website (as discussed in Chapter 2).

The 1996 Federal Health Insurance Portability and Accountability Act (HIPAA) requires healthcare providers, health plans and healthcare clearinghouses to allow you to access your medical records. Notices you receive from providers and plans must include information about how to obtain them as well as the fees charged for receiving the copies.

To obtain a copy write to: U.S. Department of Health and Human Services

Office of Civil Rights
200 Independence Avenue, S.W.
Washington, D.C., 20201
Phone: 1-866-627-7748
Web: *www.hhs.gov*

The Medical Information Bureau (MIB) is a central database of medical information shared by insurance companies. Approximately 15 million Americans and Canadians are on file in the MIB's computers and about 600 insurance firms use the services of the MIB primarily to obtain information about life insurance and individual health insurance policy applicants.

The MIB database contains information the insurance companies receive when you apply for life or health insurance as an individual. This can be the information you put down on forms, the results of blood and/or urine tests, medical

conditions the insurance companies deem as significant and lifestyle choices.

The information is not listed as specific conditions, but as codes. Examples include codes to indicate high blood pressure, asthma, diabetes or depression. A code can signify participation in high-risk sports such as skydiving. A file would also include a code to indicate that the individual smokes cigarettes. The MIB uses 230 such codes.

It's important to remember the following about the MIB:

- The MIB is *not* subject to HIPAA. MIB files do not include the totality of one's medical records as held by your healthcare provider.
- A decision on whether to insure you is not supposed to be based solely on the MIB report.
- The MIB is a consumer reporting agency subject to the Federal Fair Credit Reporting Act (FCRA). If you are denied insurance based on an MIB report, you are entitled to certain rights under the FCRA, including the ability to obtain a free report and the right to have erroneous information corrected. See the Federal Trade Commission's website *(www.ftc.gov)* on insurance decisions.

The MIB does not have a file on everyone. But if you have an MIB file, you will want to be sure it is correct. You can obtain a copy for free once a year by calling 1-866-692-6901 (TTY for the hearing impaired 1-866-346-3642) or by visiting the MIB's website.

In general the MIB can be contacted at:

Medical Information Bureau
P.O. Box 105
Essex Station, Boston, MA 02112

You can also send an email to *infoline@mib.com* or visit

MIB on the web at *www.mib.com.*[34]

If you believe your EHR contains inaccurate information or your privacy has been violated, you can petition to get the information removed. HHS has information on how to file a complaint on its website *www.hhs.gov/ocr/privacy/hipaa/complaints/index.html.* In short, complaints must be submitted in writing and mailed or faxed to one of 10 regional offices.

Paying cash for health services—rather than using health insurance—and finding a healthcare practitioner who does not require you to give your Social Security number will go a long way towards helping maintain your medical privacy. But it's still no guarantee. However, taking your healthcare business abroad will keep you out of the U.S. system.

The practice is called medical tourism and it can be far more beneficial than just protecting privacy. Many hospitals in places like New Zealand, Thailand, India, Mexico and Costa Rica cater to wealthy foreigners. The physicians there are often trained in the U.S. and the care the hospitals provide is as good as or better than what you find in America… and often less expensive. You can also often get access to drugs and treatment options not approved in the United States.

There are several companies that help arrange offshore medical visits. These help to ensure that you select the best doctors and facilities. There are also volunteer organizations that certify the foreign facilities. One of these is Joint Commission International *(www.jointcommission international.org).*[35]

CHAPTER 7

Putting the Genie Back in the Bottle… Sort of

The Founding Fathers recognized that an oppressive government could use its powers to intimidate, harass or steal the possessions of average citizens. In fact, British royal officers would use "writs of assistance" to conduct searches of the homes of colonists in an effort to detect violations of British customs laws. So the 4th Amendment to the Constitution was passed which says, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable search 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."

Yet today the Federal government tramples all over the spirit, if not the letter, of the 4th Amendment with its USA PATRIOT Act, FinCEN, SAR, CTR, TIA and ADVISE programs. Bureaucrats, businesses and crooks alike are mining the data of millions of Americans looking at what you read, what you buy, where you shop and what you eat, and making a determination about you and your character based on the information a computer kicks out.

Government spooks are now pushing for new, expanded police powers that will include mandatory fingerprinting, iris

scans and DNA sampling of all citizens, national biometric ID cards, transponder tracking of vehicles (some politicians are advocating a mileage tax) and even geographical tracking of citizens through microchip implants.

And even though it may not be happening now, in the very near future you could see discrimination, profiling or harassment resulting from all the information stored in government computers. Don't think so? Ask the Japanese, some of whom are experiencing "bura-hara," which is blood type harassment.

Based on what many call sham science, many Japanese are being segregated based on their blood type, even though doing so is supposedly against Japanese law. The theory is that a person's personality, work ethic and morals can be determined by blood type. It is affecting children in kindergarten, and the Japanese women's softball team members had their training regiments personalized based on their blood type.

Any information in your electronic database could set off "flags" or could be pulled out and used against you at any time and for any reason. And if you have the courage or occasion to speak out against your government, some vindictive member of the person's staff may very well be into your files looking at your records for a way to slime your reputation. That's what the Obama campaign team and the mainstream media tried to do to Joe "the Plumber" Wurzelbacher, who saw his life exposed and his reputation sullied simply because he responded to a Presidential candidate during a chance encounter.

What Can You Do About it?

One thing you can't do is completely put the genie back in the bottle. If you have been using credit cards, debit

cards or loyalty cards, or you have rented movies or given out your Social Security number or if you have a cellular telephone or other wireless device, you are in the database. The watchers have your information. Private investigators, vindictive spouses, greedy lawyers or jilted lovers (real or imagined) can learn all about you and possibly track you down.

However, that doesn't mean they have to have your latest information. You can begin now to make it more difficult to be tracked or found.

When making a purchase, do so with cash. If you feel you must have a credit card for emergencies, or to make online purchases, don't sign up for more credit accounts than you really need. For most people, a major credit card—two at most—and perhaps two or three cards from department stores or other retailers will provide all the credit and flexibility that they need. If you have dozens of credit cards, consider cutting some of them up. When you



do, be sure to also call or write the issuing companies to cancel your accounts individually.

In his book, *Privacy Crisis,* Grant Hall recommends using credit cards to pay large bills if the company agrees not to retain your name and credit card information in their database. He says that some large companies are willing to do this—if you speak with a company manager in advance —but smaller companies are usually reluctant.

Hall says a better way to make purchases electronically is to use a pre-paid debit card that has the VISA or MasterCard logo stamped on it. Those accounts can be opened without having to provide personal details and the cards can be funded with cash payments. That way, no electronic trail is left that leads back to you.

Another secure method of paying bills or buying things is through the online payment service PayPal *(www.paypal.com).* When you set up a PayPal account, it is associated with your bank account, credit card or both. This allows you to send money to another PayPal account holder anonymously. The funds are either withdrawn from your bank account or charged to your credit card, or they can be deducted from funds deposited directly to your Paypal account.

When you make a transaction through PayPal, none of your personal financial information is revealed to the other party involved in the transaction or to your financial institutions. If the money for the payment comes from your checking account the bank statement will list the payment as "PayPal E-Check." If the payment comes from your credit card, the statement will list the payment as "PayPal." The person receiving the payment will not know which bank or credit card your payment comes from and will not see any personal information that a check might reveal (like name, address, telephone number

and banking account number).

Any competent investigator—private or public—will be able to obtain information about your financial records by developing sources inside the bank or by using pretexting methods (private) or through the use of subpoenas (public). But using PayPal—which has a very strict privacy policy and has shown no sign of compromising it—creates a buffer that prevents disclosure of your activities.[36]

To bank anonymously, Hall recommends setting up a revocable trust and opening a non-interest bearing checking account in an American bank. He describes in detail in his book how to set up the trust account. The following is a summation:

First, you as trustee or someone else as administrative trustee must file Form SS4 with the IRS to receive an Employer Identification Number. Since a company tax identification or Social Security number must be included on the form, this does give a paper trail to the IRS. However, since you are going to open a non-interest bearing account, no Form 1099 will be generated and the IRS will neither know nor care about the trust.

Second, create your trust with a name that has no similarity to your true name. You can employ the services of an attorney to set up the trust or use a legal-forms store or online service. A trust is better for banking privacy than a corporation or LLC because there is no registration requirement to establish a trust. Also, business entities are designed to separate personal and business money and assets while a trust can be used for the deposit of checks to the trustee or trustees, individually or to the trust itself.

Next, open a non-interest bearing checking account in the trust's name with yourself and whoever else you

designate as signers of the account. The bank will recognize your signature on any checks written, but the owner of the account will be the trust. With a trust account no investigator trying to find you can trace the transactions back to you.

A trust can also help your heirs inherit more of your estate and avoid probate after your death. Probate involves inventorying and appraising the property, paying debts and taxes, and distributing the remainder of the property as outlined in the will. However, if a living trust is formed, surviving heirs can transfer the property quickly and easily. And, because of the way a trust is structured, the property can avoid estate taxes.

There are two types of trusts available for this strategy, the living trust and the AB trust, and the one that best suits you is determined by the size of the estate and your personal circumstances. You should seek the advice of an attorney when considering this strategy because each person's situation is different and Congress is always tinkering with tax laws.

A trust can also help protect your home if you are a party to a lawsuit or get into trouble with the IRS. Even more home protection can come from placing your home in the name of a limited liability company (LLC). By using a single-member LLC you don't run afoul of tax laws requiring you maintain residence in the home to keep your homestead exemption. However, if you become party to a lawsuit or if the IRS tries to seize your property to settle a tax debt, the house is protected because it is owned by the LLC rather than you as an individual.

Two other entities you can establish are Family Limited Liability Companies and Family Limited Partnerships.

Family LLCs or Family Limited Partnerships are great tools for protecting your assets from creditors. You can put your investments in such an entity, and prevent a creditor from seizing the assets in your Family LLC or Family Limited Partnership in the event you are sued. But these steps need to be taken before a situation arises in which a creditor or other legal predator comes after your assets. Attempting to hide them once the legal process is underway can be considered a "fraudulent conveyance." If you try to move assets into an asset protection structure after a creditor situation arises (or even after the potential for a creditor situation arises) it's likely too late. Any transfer would be considered a fraudulent conveyance, and a court could unwind the transaction and give the assets to your creditors.[37]

A fraudulent conveyance falls under the Uniform Fraudulent Transfers Act (UFTA), which is the law in 41 States. In essence, the UFTA stipulates that if property is transferred to "hinder, delay, or defraud" an existing or known future obligation, the courts can void the transfer. If a creditor can demonstrate "badges of fraud" associated with a transfer, the court may require you to prove the transfer wasn't intended to hinder, delay or defraud. Badges of fraud include:

- Making the transfer to an insider.
- Retaining use or control of property.
- Concealing the transfer.
- Being sued or threatened with a lawsuit.
- Making a transfer of substantially all of your assets.
- Absconding.
- Removing or concealing assets.
- Becoming insolvent shortly after making the transfer.

- Not receiving reasonable value in return for transferred assets.
- Making the transfer shortly before or shortly after a substantial debt was incurred.

One badge of fraud won't ordinarily demonstrate fraudulent conveyance. Where several are present, the court my set the transfer aside and order payment of the debt.[38] Be sure you consult an attorney for full information on laws particular to your State and circumstance.

If this seems like more trouble than you want to go to, at least limit the information you have printed on your personal checks and use them only to make routine payments to established accounts like utility bills, loan payments, etc. You can use an initial and your last name rather than your full name. Never put any other information—your address, telephone number, SSN or driver license number—on your check. And never have your checks delivered to your home mailbox. Always go to the bank to pick them up.

Possessing that information makes it simple for a ne'er-do-well to learn how much money is in your account and set up bogus accounts in your name.[39]

For in-store purchases, use a prepaid debit or credit card rather than check.

Never give out your Social Security number except when necessary on government forms like tax returns. Question every request you get to provide your number and try to negotiate an alternative such as a driver license, suggest David H. Holtzman in his book, *Privacy Lost.*

If you are concerned about being tracked, avoid using modern technology like cell phones, a global positioning system or similar items. If you have a cell phone, take out

the battery when you're not using the phone. Cell phones have essentially become tracking devices. They constantly send out signals to nearby towers. It takes the cell phone companies just minutes to triangulate the position of the cell phone based on its signal to the nearest three towers.

Find out whether your vehicle has GPS technology of some kind built in—many newer ones do—and trade vehicles or have the GPS disabled if possible, according to Holtzman.

If you feel a cell phone is a must, use a prepaid cell phone. There are many now that don't require a contract or credit check—TracFone, Net10 and AT&T's GoPhone are good ones to consider—and they are perfect for someone wanting to maintain privacy. The retailer may ask for a billing address, but it is not necessary to provide one, so use your discretion about what information you provide.

Because prepaid cell phones are so discreet—and disposable—the government would like to ban their use. Attempts to move such laws out of committee have thus far failed.

Become Someone Else

It requires some effort and time, but it's possible to become someone else. In other words, you can establish an alternate identity for yourself if you need to drop off the radar. Doing so requires thoughtful planning if you're going to pull it off. But the new "person" can enjoy all the privileges of the old person without the fear of someone tracking you down that you don't want to find you.

When planning an alternate identity, it is first necessary to sit down with a piece of paper and map out a life history. Name, date and place of birth, parent's names (including a maiden name for your mother), education and occupation (current and prior employment) are all issues to consider.

The name you choose should be a common one—to make it easier to blend in with the crowd. You should keep your birth date near your actual one for plausibility. It's best to choose large metropolitan areas with a lot of bureaucracy and people as your place of birth. A good alternate identity will easily blend into a crowd and get lost in a confused bureaucracy. The mother's maiden name is a common question on applications and is often used to establish one's identity. Again, a common one is better.

You should establish a new mailing address, and there are several ways this can be accomplished. It's not as simple as going to a local Mail Boxes, Etc. store and asking for a post office box because you need two pieces of identification, one of which is a photo ID. So here are some alternative suggestions.

If you live in or near or have access to an apartment complex with multiple mailboxes, it's possible to secure a used one to begin receiving mail. If you live in a rural area, it might be possible to mount a mailbox on a post with multiple mailboxes and create a new address. If you do this, be sure the new house number you create does not already exist.[40]

And there are other ways to establish a new address, but they often require a little more creativity and gumption. One is to locate an old commercial building that caters to a number of businesses but has multiple vacancies or is undergoing renovation. Locate the owner or leasing agent and explain that you own a small business that needs a location for occasional mail and package deliveries but have no need of office space because you're usually out of town. Sometimes, if your story is convincing enough and you dress the part, for a small fee you can get the owner to "lease" you some space

with a mailbox with few questions asked.

This sort of arrangement has also worked in buildings with no vacancies by offering to pay a rental fee for a small portion of storage space like a broom closet.

Small motels and businesses that proved office services, bookkeeping services and other professional services are also good places to inquire. With a convincing story and the offer of cash up front, you can accomplish a lot.[41]

If your desire is just to lay low, you can now use the new mailing address and receive all correspondence using only your first and middle names or the name of your established trust or LLC.

If what you want is simply to establish for yourself a new address—and not an entirely new identity—you can also use these methods as well. Once your new address is established you can use the postal address change form to divert your mail from your old address to the new. Then look around your house and notice what makes it look like "you" live there. Make changes to erase any sign of "you" and add things to make it look like someone else is living there.

However, if you're working on a new ID, once you've established your new address, it's time to proceed with bulking up your identity. You can subscribe to a magazine (paid for by money order) and register with various "people finder" services on the Internet. You should create an email account or two with your alternate identity. You can apply for shopper preference cards or take membership in a "buyer's club." The idea is to provide yourself with ID cards that don't require presenting ID to acquire them.

The next task is to get a primary source of identification which means a "government-issued" photo ID. A SSN is

almost always required when filling out important documents. While you could always just select a number out of thin air, there is the likelihood that the one you pick belongs to a living person and the possibility that you could pick one associated with a known criminal or worse, an IRS agent. In these cases you could be guilty of committing identity theft or find yourself charged with crimes you didn't commit.

A safer bet is to use what has become known as a "pocketbook SSN." These are numbers that have been taken out of circulation for one reason or another. They are not and never have been assigned to anyone. A list of these numbers can be found by using a search engine to search the term "pocketbook SSN" (be sure you use a secure search method as discussed on page 55). It's best to pick one from the same State you selected as your new birth State.

Using your new SSN to acquire a new driver license can be a tricky proposition. Depending on the level of bureaucracy, the busyness of the office and the conscientiousness of the employees, your SSN might be checked. Therefore it's best to either buy or make one. There are books available that provide step-by-step instructions on how to do it. It also requires a computer and a good printer.[42]

There are also a number of websites that will make novelty IDs for a price. These can be found with an online search.

Erasing Vestiges of the "Old" You

Go to a popular search engine like Google, enter your name and click "search." You might be very surprised—and a little concerned—at all the information about you

that is easily obtained. It's going to take some time, but you can begin to slowly, but surely, erase your personal information from most public databases.

Begin by going to the search pages listed with your name. Most of them will have an "opt-out" option you can use to remove the information that page has. Key systems that may also have your address, telephone number and other information include:

- *AnyWho.com*
- *PhoneNumber.com*
- *Switchboard.com*
- *YellowPages.com*
- *Zabasearch.com*
- Google's various services.

A little time spent tracking down online information about you and your family members and getting the data removed will greatly increase your privacy, and might even save you a lot of time and money. In an age of stalkers and other criminal activity, it could even save your life.[43]

Think that's extreme? Public records aggregation websites like *PeekYou.com*, *BeenVerified.com* and *Docusearch.com* search the web and government public records databases for information. As Docusearch advertises, "Our most popular searches: Looking for the owner of a vehicle by plate # or VIN? Trying to locate someone's SSN? Want to a reverse telephone number? Looking for someone? We have several ways you can search and all our resources are up to the minute."

Apparently it delivers on its promise. I mentioned on page 33 the case of Amy Lynn Boyer. She was killed

as a result of public information about her obtained by Docusearch.

On July 29, 1999, Liam Youens contacted Docusearch and requested Boyer's date of birth. He later contacted Docusearch and obtained her SSN and employment information. For this he paid $45. Docusearch then hired a woman name Michelle Gambino to make a "pretext" call to Boyer at her workplace. Gambino pretended to work for Boyer's insurance company and said that she needed some information verified, including the address of Boyer's office, to refund an overpayment. This information was then given to Youens $109.

On Oct. 15, 1999, Youens drove to Boyer's workplace and shot her to death as she left the office. He then killed himself.[44]

With all the crazies in the world and database sites like Docusearch that allow anyone access to your motor vehicle registration information, the simple act of accidently cutting someone off in traffic could be a death warrant. For less than $100 a vindictive motorist can learn where you live, where you work and whether you have a gun permit.

Battered spouses, victims of stalking and survivors of sexual assault are now getting a little help from their governments. Some States have initiated what are called "Safe at Home" programs to help people "disappear." While not witness protection programs, they are designed to help victims hide in plain sight by providing free post office box and mail forwarding services, confidential name-changing services, confidential voter registration, suppression of Department of Motor Vehicle records, and assistance with removing all identifying information from the Internet and government databases. Not all States have

this service, but those that do can give you a leg up on "erasing the old you."

Women fleeing from abusive stalkers and others who value privacy sometimes ask their roommates, friends or family to set up the utility and cable bills for them. As long as the bills are paid, the utility companies will be happy. Also, some States allow attorneys, business managers and others to set up and pay for such utilities for their clients. Check the laws in your State to make sure everything you do is legal.

If you don't fit into the battered spouse category but still want to "disappear," there are other steps you can take that will throw the most determined searcher off your trail: Register your car under the name of a limited liability corporation (LLC).

To limit the paper trail available you should always purchase cars with cash. Sign the bill of sale under the name of the LLC which is also registered in a State other than the one in which you live. If a signature is required on the bill of sale, make it as illegible as possible. You can register the car in a State other than one you live—and other than the one in which the LLC is registered—by claiming that you will be a resident of the State for six months. State laws require any vehicles that will be in a State for six months or more be registered in that State.

By using this sleight of hand, a determined psychopath or private investigator will have a devil of a time tracking you down because your name and address are in no way connected to the vehicle.

You can use this same method for buying real estate that you want to keep private.

When insuring your vehicle, do so under your first initial and last name with a doing business as (dba) using the name of your LLC. This will also make you very difficult to find through a trace of your vehicle's license plate number.[45]

Some Final Thoughts on Privacy

This is not an all-encompassing book on the issues of privacy. First of all, covering or attempting to cover every aspect of privacy in one book is impossible. There are too many variables in people's lives. Technology is constantly changing. Laws are changing too, but governments are often slow to react and the courts—while typically favoring government in most privacy cases—are still grappling with whether it is legal for citizens to record the public actions of police officers. Expecting the courts and government to deal with stickier matters of personal privacy—or at least deal with them coherently and in a way that protects our rights as Americans—is out of the question. After all, the government's agenda is toward less individual privacy, not more.

So I have provided you with both a bibliography and a list of references. These can provide you with more information on a subject we may have touched on just briefly—or not all. But hopefully this book has given you plenty to think about and a good start as you make your own personal privacy plan. And remember privacy is a process rather than a destination. As soon as you think you have covered all aspects of personal privacy, some new technology will come along or a new law will be passed that will undo your hard work.

References

1 http://searchsecurity.techtarget.com/definition/Tempest

2 http://mashable.com/2012/07/12/facebook-scanning-chats/

3 http://personalliberty.com/2012/07/16/terror-perverts-and-big-brother/?eiid

4 http://www.fas.org/irp/eprint/rightwing.pdf

5 http://www.courierpress.com/news/2012/jun/22/swat-team-enters-home-people-inside-arent/

6 Duncan Long, *Protect Your Privacy* (The Lyons Press, 2007), p. 123.

7 Long, P*rotect Your Privacy*, pp. 177-178.

8 Michael Chesbro, *The Privacy Handbook* (Paladin Press, 2002), pp. 50-53.

9 Long, *Protect Your Privacy,* pp. 144-145.

10 Long, *Protect Your Privacy,* pp. 165-166.

11 http://www.makeuseof.com/tag/opendns-works-as-a-great-free-content-filtering-solution/

12 Chesbro, *The Privacy Handbook,* pp. 24-25.

13 Chesbro, *The Privacy Handbook,* pp. 27-28.

14 Chesbro, *The Privacy Handbook,* pp. 39-40.

15 http://abcnews.go.com/blogs/politics/2012/05/senators-to-unveil-the-ex-patriot-act-to-respond-to-facebooks-saverins-tax-scheme/

16 http://www.jensenestatelaw.com/articles/trusts/250-spousal-gift-trust

17 Long, *Protect Your Privacy,* p. 5.

18 Chesbro, *The Privacy Handbook,* pp. 157-158.

19 http://fortresssecuresolutions.com/thirdparty.html

20 Chesbro, *The Privacy Handbook,* p. 154

21 http://www.thepreparedninja.com/21-things-a-burglar-wont-tell-you

22 Chesbro, *The Privacy Handbook,* pp. 88-89.

23 http://www.zdnet.com/blog/networking/beyond-skype-voip-alternatives/1061

24 http://www.techinfoblog.net/voip-encryption-make-sure-your-phone-calls-are-protected/

25 http://www.washingtonpost.com/business/economy/skype-makes-chats-and-user-data-more-available-to-police/2012/07/25/gJQAobI39W_story.html

26 http://www.pimall.com/nais/cellphonebox.html

27 http://www.cellutips.com/7-tips-to-help-protect-your-cell-phone-privacy/

28 http://personalliberty.com/2012/05/21/why-it-doesnt-pay-to-cooperate-with-police/

29 http://news.cnet.com/8301-13578_3-10161233-38.html

30 http://www.news-medical.net/news/20111024/Your-medical-privacy-e28093-Another-Obamacare-casualty.aspx

31 http://www.givemebackmycredit.com/blog/2010/02/cancer-patient-identity-theft-victims-day-in-court-hangs-on-supreme-court-decisions-1.html

32 http://www.rawstory.com/rs/2010/09/08/cops-access-drug-prescription-records/

33 http://patients.about.com/od/costsconsumerism/f/doctors requestssns.htm

34 https://www.privacyrights.org/fs/fs8-med.htm

35 http://www.howtovanish.com/2011/09/patient-privacy-rights-and-private-hospitals/

36 Chesbro, *The Privacy Handbook,* pp.17-18.

37 http://www.nuwireinvestor.com/articles/asset-protection-in-uncertain-times-58587.aspx

38 Mark Nestmann, *The Lifeboat Strategy: Legally Protecting Wealth and Privacy in the 21st Century,* 3rd Edition 2007-2008 (The Nestmann Group, Ltd., 2003).

39 Chesbro, *The Privacy Handbook*, pp. 35-38.

40 Chesbro, *The Privacy Handbook,* pp. 169-171.

41 J.J. Luna, *How To Be Invisible* (Thomas Dunne Books, St. Martin's Press, 2004), pp. 63-65.

42 Chesbro, *The Privacy Handbook,* pp. 167-178.

43 Long, *Protect Your Privacy,* pp. 181-182.

44 http://epic.org/privacy/boyer/

45 Luna, *How To Be Invisible,* pp. 182-189.

Bibliography

Everything I Want to Do is Illegal: War Stories from the Local Food Front, by Joel Salatin (Polyface, 2007)

The Lifeboat Strategy, by Mark Nestmann (The Nestmann Group, Ltd. 2003, Third Edition, October 2007)

Three Felonies a Day: How the Feds Target the Innocent, by Harvey A. Silverglate (Encounter Books, 2009)

Privacy Crisis, by Grant Hall (James Clark King, LLC, 2006)

Privacy Lost, by David H. Holtzman, (Jossey-Bass, 2006)

Protect Your Privacy, by Duncan Long (The Lyons Press, 2007)

The Privacy Handbook, by Michael Chesbro (Paladin Press, 2002)

Index

AT&T's GoPhone 133

1996 Federal Health Insurance Portability and Accountability Act (HIPAA) 122, 123

4th Amendment 112, 125

7th Circuit of the U.S. Court of Appeals 111

A

AB trust 130

ACLU 43

ADT® 94

advertising 15, 17

advocacy groups 43

al-Qaida 65

Alabama 107

algorithms 13

alternate identity 133, 134, 135

American College Test (ACT) 24

Americans 17, 27, 63, 76, 83, 85, 122, 125, 140

Analysis, Dissemination, Visualization, Insight and Semantic Enhancement (ADVISE) 69, 125

anti-money laundering 60

AnyWho.com 137

AOL 54

assets 15, 16, 83, 84, 85, 87, 88, 129, 131, 132

asthma 123

ATM 70

Australia 12

Avera, Diane 106, 107, 108

AVG 45

B

babies 18

backscatter radar 15

bank 14, 20, 39, 46, 54, 59, 60, 61, 63, 64, 65, 66, 71, 76, 77, 80, 81, 82, 83, 84, 117, 128, 129, 130, 132

Bank Secrecy Act 63

bar codes 36

barter clubs 72

BCWipe 53
BeenVerified.com 137
beneficiary 85, 86
BetterPrivacy 55
Big Brother 11, 17, 88
binary 58
biometric scanning 17
BIOS password 51
Bit Wise 56
black boxes 41, 42
blogged 47
blood type harassment 126
Bluehost.com 56
Boston Police Department 32
Boyer, Amy 33, 137, 138
British royal officers 125
broker 20, 33, 61
browser 46, 49, 51, 55, 56, 57
bureaucrats 8, 16, 22, 27, 73, 125

C

California 42, 99
call forwarding 102
caller ID 101, 102
cameras 15, 21, 22, 23, 101, 110
Canada 12, 56
Capitol Hill 82
Carnivore 12
Casey, Bob 81
cash value 85, 86, 87
CasperTech 55
CBP 44
Cellular 98, 100, 121, 127
Central Intelligence Agency (CIA) 44, 63, 64
Centurion 54
certified mail 75
cervical cancer 116
Charlotte News & Observer 118
Chicago 48
China 44
Christian Science Monitor 69
Cisco Telepresence 101
Clinton, Bill 54, 118
cloud storage 113
Cnet.com 115, 142
CNN 35
CNNMoney.com 70
Communications Assistance for Law Enforcement Act (CALEA) 21
Computer Fraud and Abuse Act 26, 27
computer scoring 71
Congress 47, 74, 81, 82, 118, 119, 130

cookies 49
copyright violation 47
cordless 98, 100, 121
Costa Rica 124
credit card 14, 29, 38, 39, 59, 61, 69, 71, 76, 77, 80, 101, 103, 117, 120, 126, 127, 128, 132
credit report 62, 63, 78, 80, 117, 120
creditors 77, 78, 86, 131
crime 11, 23, 26, 27, 67, 78, 117, 136
criminal 8, 17, 18, 32, 54, 60, 89, 136, 137
CRT monitor 14
Crypto Heaven 56
crystal methamphetamine 108
currency transaction report (CTR) 20, 65
CVS 107

D

data mining 15, 69, 70, 76
data traffic 12
date of birth 32, 59, 120, 138
DEA 59
Defense Intelligence Agency 70
Democratic 26, 27
Department of Defense 117
Department of Justice 26
Department of Motor Vehicle 138
depression 123
diabetes 123
digital fingerprint 29
digital telephones 100
digitalDNA 24
discount store cards 39
divorce 26
DNA 17, 18, 19, 24, 126
Docusearch 33, 137, 138
Docusearch.com 137
Drew, Eric 117
driver's license 34, 59, 110, 119, 132
Drones 21, 23
DWIPER 53

E

e-file system 75
Eagle's Eye program 66
Echelon 11
Ekiga.net 101
Eldridge, Michelle 70

Electronic Privacy Information Center (EPIC) 70
electronic transmissions 14
electronically 27, 74, 75, 76, 128
email 12, 46, 52, 53, 54, 88, 113, 123, 135
Employer Identification Number 129
EMR 12, 13, 14
encrypting 51
Equifax 63, 78
Eraser 53
event data recorders 41
Everything I Want to do is Illegal 8, 143
Ex-PATRIOT 81
expatriates 82
Experian 63, 78

F

Facebook 16, 17, 29, 30, 31, 32, 35, 36, 55, 81, 98
Facetime 101
Family Limited Partnership 130, 131
Family LLC 131
Faraday 14, 39
Faraday Box 39
faxes 12
FBI 32, 55, 59, 64, 67
Federal Aviation Administration 23
Federal code 8
Federal Fair Credit Reporting Act (FCRA) 62, 123
Federal Suspicious Activity Report (SAR) 63, 64, 125
Federal Trade Commission 76, 77, 80, 123
FedEx 36, 68
FEMA 44
Financial Crimes Enforcement Network (FinCEN) 20, 59, 60, 64, 76, 125
fingerprints 19, 60
Fire 56
Firefox 55, 56
firewall 46
Florida 32, 35
Florida's Holy Name Monastery 65
foreign bankers 81
foreign countries 81
Form 1099 71, 129
Form SS4 129
Forms W-2 71

fraud 26, 27, 35, 77, 78, 80, 85, 131, 132
fraudulent conveyance 131, 132
Free Internet Window Washer 3.1 57
Freedom of Information Act 70
freeware 50, 52, 53, 54
friend list 31
friend requests 31

G

Gabreski Airport 105
Gale 56
Gambino, Michelle 138
Gardiner, Richard 109
General Dynamics 44
Genovese, Nancy 105
Germany 56
Ghostery 55
Gmail 15, 54, 113
Gold Lock 55
Google 15, 16, 17, 49, 54, 55, 136, 137
Google Android phones 55
Google Chat 101
Google Talk 101
Google Voice 101, 102
government snoops 7, 20, 55, 69, 82, 98, 99
GPS 14, 101, 104, 133
Gramm-Lech-Bliley Act 60, 61
Great Britain 12

H

Hall, Grant 128
Hawaii 25
health insurance 115, 121, 122, 124
high blood pressure 123
Hilton, Paris 50
Holtzman, David H. 132, 133
home invasion robberies 89, 90
home security system 94
human papilloma virus (HPV) 116
Hushmail 54

I

ICE 44
iCloud 53
identification numbers 33
identity 33, 76, 77, 80, 103, 133, 134, 135, 142
identity cards 17, 19

identity theft 76, 79, 80, 117, 136
identity thieves 61, 76, 79
Image Data 34
India 44, 124
input-output system 51
Instant Messaging (IM) 54, 56
Instant Messengers 57
insurance 41, 42, 61, 82, 83, 84, 85, 86, 87, 115, 120, 121, 122, 123, 124, 138
insurance companies 18, 41, 42, 82, 85, 120, 122, 123
insurance fraud 26
IntelliScript 120
Internet 12, 21, 25, 26, 29, 32, 34, 45, 47, 49, 50, 54, 57, 90, 101, 102, 135, 138
Internet Archives 35
Internet Protocol (IP) address 32, 47, 55
Internet service provider (ISP) 25, 47
iPad 53
iPhone 53
ippi 101
Iptel 101
iris scans 19, 125
IRS 19, 59, 60, 64, 65, 70, 71, 72, 73, 74, 75, 76, 83, 84, 85, 86, 118, 129, 130, 136
IRS Restructuring and Reform Act 74
Italy 49

J

Japanese 126
Jett, Robert 89, 90, 93
Joint Commission International 124
judges 8
junk mail 62
juvenile 18

K

Kathleen Romano v Steelcase Inc. 35
Kept Private 54
KeyKatch 51
KeyScrambler Personal 51
keywords 15
Kim, Augustine 106, 108, 109

L

lawyers 8, 61, 82, 86, 127
leaked 61
Libertarian Party 44

license plate 14, 110, 140
life insurance 83, 84, 85, 86, 87, 120, 122
limited liability company (LLC) 129, 130, 131, 135, 139, 140
line blocking 102
living trust 130
login 31, 32, 50, 113
London 21
loyalty cards 39, 127

M

Mac 56
Mac Mail 113
Macintosh 48
Mail Boxes, Etc. 134
marketers 29, 34, 61
MasterCard 128
McAfee 45
Medco High Security 94
Medicaid 115
Medical Information Bureau (MIB) 122, 123, 124
medical records 24, 40, 115, 117, 118, 119, 121, 122, 123
Medicare 115
MedPoint 120
methadone 108
Mexico 124
microphones 15, 22
Microsoft Office 57
Microsoft Outlook 54
Middle East 44
military 44, 55, 60
Minnesota 19
misdemeanors 18, 27
Mississippi 107
Missouri 31, 43
Mizuno, Rep. John 25
Modernhealthcare.com 117
money 14, 15, 17, 20, 38, 44, 47, 60, 63, 64, 66, 67, 70, 72, 76, 81, 82, 83, 89, 90, 97, 128, 129, 132, 135, 137
money laundering 14, 60, 63
money orders 20, 66, 67, 68
motor vehicle registration 138
movies 47, 127
MSN Mobile 104
Mute Mail 54
Mutilate File Wiper 53
MySpace 27, 35, 36

N

Napster 47
National Security Agency (NSA) 21, 70
National Security Council 59
Nestmann, Mark 109, 111, 142
Net10 133
New Jersey 106
New York 35, 105
New York City 21
New Zealand 12, 124
News-medical.net 116
Nixon, Richard 118
North Carolina 106, 117, 118
North Dakota 23

O

Obama 27, 126
Obamacare 115
offshore 56, 70, 81, 82, 83, 84, 124
offshore insurance policy 84
Oklahoma City 89
OnTrack Automotive Accessories 110
OoVoo 101
OpenDNS 57, 58
Orwell, George 11
Outlook Express 57
OxyContin 118

P

paperless 74
passport 34, 38, 39
password 31, 50, 51, 58, 79, 80, 81, 103, 104, 111
password safes 50
Patient Protection and Affordable Healthcare Act 115
Paul, Ron 44, 66
PayPal 128, 129
Paypal Mobile 104
PCworld.com 49
PeekYou.com 137
Pennsylvania 35
Pentagon 69, 70, 117
Pentagon's Total Information Awareness 69
Percocet 118
personal identification numbers (PINs) 79
phishing 46, 58, 77
phone taps 100
PhoneNumber.com 137
photo ID 34, 134, 135

PhotoBlocker Spray 110
pocketbook SSN 136
police 7, 8, 14, 15, 22, 23, 26, 32, 41, 42, 47, 48, 78, 90, 91, 92, 94, 95, 105, 106, 107, 108, 109, 110, 111, 125, 140
police scanners 110
politicians 19, 22, 27, 41, 72, 118, 126
post office box 68, 134, 138
Predator drone 23
prepaid calling cards 102
privacy 136, 137, 138, 139
Privacy Crisis 128
Privacy Lost 132
Privacy Rights Clearinghouse 120
privacy settings 29
private detectives 7
private investigators 61, 69, 84, 127
probate 86, 130
prosecutor 8, 26, 27, 108
protective intelligence bulletin 43
pseudoephedrine 107
Psst 56
public domain 31

Q

QR codes 36

R

radar detectors 110
radio frequency identification (RFID) 37, 38, 39
radio scanner 100
red flags 72, 73, 119
Red Flags Rule 119
red light camera 22
registered mail 75
Report of International Transportation of Currency or Monetary Instruments 67
Republican 26, 27, 44
Roosevelt, Franklin Delano 118
Russia 46

S

Safe at Home 138
Salatin, Joel 83
Saverin, Eduardo 81, 82
scanner 37, 38, 40, 100
Schumer, Chuck 81
Scholastic Aptitude Test (SAT) 24
search engines 49, 53, 55, 102, 110, 136

Secretary of the Treasury 20
Secure Real-Time Transfer Protocol (SRTP) 101
Secure Shuttle 56
Securenym 54
shredders 80
skimming 77
Skype 21, 101
smart meters 99
smartphone 36
Social Security Administration 33
Social Security number 32, 33, 59, 79, 80, 81, 118, 124, 127, 129, 132
Sonork 56
Soronen, Tim 107, 108
South Carolina 106
Spain 56
SpectorSoft 51
speed traps 110
Spousal Gift Trust 87
spread spectrum 100
Spy Exchange & Security Center 101
StartPage 55
State Department of Human Resources 108
State Department's Bureau of Intelligence and Research 59
Strait, Bob and Nancy 90
structuring 66, 67
Sudafed® 107, 108
sdurfing 45, 55
surveillance 11, 15, 21, 23, 42, 55, 70, 99
suspicious activities 60
SWAT team 23
Swiss annuity 82, 83
Swiss franc 83
Swiss law 54
Swissmail 54, 113
Switchboard.com 137
Switzerland 54, 82
Symantec 45

T

tax cheats 11
tax gap 72
tax returns 59, 72, 74, 82, 132
Telecommunications Electronics Material Protected from Emanating Spurious Transmission 12
telephone 12, 21, 50, 56, 77, 80, 81, 89, 94, 98, 100, 101, 102, 127, 128, 132, 137

Tempest 12, 13, 14
term insurance 85, 86, 87
terms of use 27
terrorism 11, 21, 22, 23
Texas 19, 66, 101
text messages 102, 103
Thailand 124
The Discriminant Function System (DIF) 71
The Lifeboat Strategy 109, 142
The Modern Militia Movement 43
The National Journal 69
The Prepared Ninja 96
The Washington Times 109
Threat Management Division 43
Three Felonies a Day: How the Feds Target the Innocent 8
TopCrypto 55
Tor Project 48
TracFone 133
TrackMeNot 55
traffic cameras 21, 110
traffic signals 21
Trans Union 63, 78
Transportation Security Administration (TSA) 112
travel 29, 39, 42, 69, 104, 112
Treasury Department 59, 63, 64, 67
Trojan 45
Twitter 55

U

U.S. Constitution 44
U.S. Department of Health and Human Services for Civil Rights 117, 122
U.S. Department of Homeland Security (DHS) 43, 44, 55, 112
U.S. dollar 83, 84, 85
U.S. Food and Drug Administration 38
U.S. government 11, 12, 38, 44, 54, 81
U.S. House of Representatives 66
U.S. Postal Service 20, 66
U.S. Secret Service 34
U.S. Supreme Court 14
Uniform Fraudulent Transfers Act (UFTA) 131
Unreported Income DIF (UIDIF) 71
UPC codes 36
UPS 36, 68

URLs 37
US Robotics 12
USA PATRIOT Act 20, 60, 63, 64, 81, 125
USA Today 21
user agent 55

V

Van Eck phreaking 14
Veil 110
VeriChip Corp 40
Veterans Administration 117
video cameras 15, 21
virus 45, 46, 52, 116
virus protection 45
VISA 128
Visual Analytics 70
Vliet, Elizabeth Lee M.D 116
Voice Over Internet Protocol (VoIP) 21, 101

W

Wachovia Bank 64
Wal-Mart 107
Walter Reed Army Medical Center 106
warrant 17, 21, 47, 91, 98, 105, 111, 138
Washington, D.C 21, 22, 106, 122
Wayback Machine 35
white noise 102
WhoIs 56
whole life insurance 85, 87
Wi-Fi 48, 49
WikiLeaks 55
Wikipedia 57
Windows 49, 57
wire transfers 60
wireless 12, 49, 99, 127
witness protection programs 138
Woods, Christopher 90
Worker's Compensation 120
Wurzelbacher, Joe "the Plumber" 126
www.cert.org 52

X

x-ray 68

Y

Yahoo 54, 113
YellowPages.com 137
Youens, Liam 33, 138
YouTube 15

Z

Zabasearch.com 137
Zentek International 56
Zimmerman, Phil 54
Zuckerberg, Mark 29

Notes:

Notes:

Notes:

THE BOB LIVINGSTON LETTER™





Personal Liberty
Media Group, LLC

PO Box 1105
Cullman, AL 35056
1-800-773-5699

www.BobLivingstonLetter.com
www.PersonalLiberty.com

BL-PR205-12