Liberty.me

RECLAIM YOUR PRIVACY:

5 Things **You** Can Do Right Now

by Bill Rounds, Esq. & Trace Mayer, JD

Liberty.me

RECLAIM YOUR PRIVACY
FIVE THINGS YOU CAN DO RIGHT NOW

GUIDE 1.3

BILL ROUNDS, ESQ. & TRACE MAYER, JD

This PDF is best viewed using Adobe Reader. If you hare having trouble accessing the hyper-links, copy the footnote URL into your browser.

INTRODUCTION

The underlying issue is not security or privacy, but freedom of choice or coercion. With violence and intimidation, whether it arises from a foreign attack or from domestic authorities with their police-state microscopes focused on everyone's lives, the effect is the same: tyranny. Freedom of choice, that which makes life worth living, requires as a fundamental element for the individual to securely go about life without intrusion or the threat of surveillance. Where there is ubiquitous police surveillance there is the police state.

Where there is ubiquitous police surveillance there is the police state.

Therefore, if we value freedom of choice instead of coercion

and force, then we should be staunch advocates for privacy, especially when we have nothing to hide. If we are espied in all circumstances, then we are persistently under threat of being unjustly judged, criticized, corrected, punished, and even plagiarized of our own autonomy. We become wards of Big Brother, bound in the chains of coercion with the reasonable fear that, either now or when we least expect it, any action may later become evidence for some imagined wrong because the all-seeing eye observes and records the minutia of daily life.

Thus, without the ability to keep secrets, individuals lose the capacity to distinguish themselves from others, to maintain independent lives, to be complete and autonomous persons. This does not mean that a person actually has to keep secrets to be autonomous, just that she or he must possess the ability to do so.

The ability to keep secrets implies the ability to disclose secrets selectively, and so the capacity for selective disclosure at one's own discretion is important to individual autonomy as well.

We want to help you exercise your unalienable right to se-

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

In this guide, we present information that, no matter where you are on your journey toward privacy—unless you're Jason Bourne—you will find useful and actionable. These five areas are not the only categories that require diligence, but they are areas in which a lack of privacy is pervasive and must be addressed in order to maintain privacy and security.

REMOVE PERSONAL INFORMATION FROM THE INTERNET

It is true that technology is advancing to track our every move, often without our knowledge. But technology is also advancing to protect privacy in ways that were not available before. There are already many tools that we can use to protect our private information, and most of them are free and easy. Unfortunately, as Julian Assange alluded to following the release of the Spy Files, much of the technological effort is aimed at invading privacy. But, if privacy is valuable to people, more and more privacy-protecting solutions will become available.

Tattoo ink and the Internet ink are very similar.

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

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

Find the Source

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

A lot of the Internet is just a big echo chamber.

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

Most sites allow you to remove data.

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

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

- **Intelius.com**
- **Acxiom.com**
- **USsearch.com**
- **Google.com**
- **Zabasearch.com**
- **Peoplefinder.com**
- **Whitepages.com**
- **Yahoosearch.com**
- **411.com**
- **Whowhere.com**
- **Privateeye.com**
- **Infospace.com**
- **Anywho.com**
- **PublicrecordsNow.com**

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

Where Do They Get This Information?

All of these websites collect your information from a lot of places like your online profiles; public records (property ownership records, court proceedings, census data, etc.); job application or resume sites; credit reporting agencies; smartphone apps; entering a sweepstakes to get free stuff; and lots of other sources that they won't even tell you about. Data is valuable and most organizations that get it, sell it. Selling your information is what made Mark Zuckerberg a billionaire.

There are lots of ways to prevent information from ever showing up in these public sources and from showing up online. The best way is to leave personal information blank whenever you are asked to provide it. When you must share information, use a ghost address, prepaid cell phones, a business entity, and other anonymizing techniques.

When you must share information, use a ghost address, prepaid cell phones, a business entity, and other anonymizing techniques.

Removing personal information from the Internet is not perfect. Traces of your personal information online may remain for a very long time. If you already have some unwanted informational "tattoos," it's not too late. The sooner you get started removing personal information from the Internet, the better off you will be.

The sooner you get started removing personal information from the Internet, the better off you will be.

Social Networking

Facebook and other social networking sites are notorious for disregarding your privacy. Social networking, however, is a powerful tool that most people want to use. Make sure your privacy settings are as strong as they can be. If you have already submitted personal information to these sites, there is probably nothing you can do now to remove that information from their databases. You can, however, remove it from your profile.

MAINTAIN A PRIVATE ADDRESS

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

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

Renting a Private Address

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

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

Renting a house, condo, or apartment instead of buying is one of the easiest ways to keep your private information out of public records.

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

Using LLCs and Corporations to Hold Real Estate

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

In many property ownership databases, it is possible to search for ownership records by owner's name. If you own multiple properties in your own name it will be easy to create an asset profile

of you. If you own multiple properties with multiple business entities it will be much harder to create such a profile, especially if each of your business entities exist for the sole purpose of managing one property.

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

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

When someone queries the ownership of an LLC, all they will get is your New Mexico LLC. It will be a dead end.

Trusts to Hold Real Estate

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

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

If You Own Real Estate in Your Name

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

Other Tactics to Prevent Address Lookup

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

CELL PHONE SECURITY

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

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

Do not use any techniques that will violate the law. That will negatively affect your privacy.

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

Subscriber Information

When you buy a phone, your name is usually attached. You sign a contract or you make payments with a credit card, or do something else that ties all of the activity on that device to you. Keeping subscription information private prevents corrupt governments from accessing that information with or without warrants, subpoenas, or due process to silence dissidents, jail peaceful protesters, and hide abuse. It also prevents hackers and rogue employees from compromising networks

Keeping subscription information private prevents corrupt governments from accessing that information with or without warrants

and databases to steal the valuable data.

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

Published Number

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

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

Stop giving out your number or give out a fake number to people who don't really need it.

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

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

You can sign up for call forwarding that forwards calls from your public number to your private number, keeping your private number confidential. **Google Voice**[1] is a helpful, free call-forwarding service.

With **Spoofcard**,[2] it can appear that you are calling from any number you want, protecting your actual number.

Location

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

[1] https://www.google.com/voice/b/0/?setup=1&pli=1#setup
[2] http://www.spoofcard.com/

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

To prevent unwanted tracking and increase your cell phone security, you can turn your cell phone off to make sure that you aren't connecting to any WiFi, your general location isn't being triangulated, and your GPS coordinates are not being tracked. Malware can continue to broadcast location information, even when the phone is switched off, although it is not common. To prevent surreptitious tracking, remove the battery.

The cell phone can also be pinged at any time to determine its location, even if you aren't using it.

Data Stored on the Phone

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

The most basic aspect of cell phone security is securing the device itself.

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

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

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

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

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

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

Full encryption is ideal to make sure that all the data is well protected from all but the most sophisticated attacks.

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

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

- **Kryptos**[3] (iPhone)
- **CellCrypt Mobile**[4] (Blackberry, Nokia)
- **WhisperSystems**[5] (Android)

Protecting Conversations

Usually when you have a confidential call with your business partner, your spouse, your attorney, or your doctor, nobody else is invited to the conversation. Cell phone networks around the world allow governments to secretly listen in on those conversations without a warrant. Rogue employees can listen to those conversations too. There is even a slight chance that malicious software is installed on your phone to capture your voice conversations.

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

Although it is still rare, phones can be infected with viruses and malware.

Although it is still rare, phones can be infected with viruses and malware, just like a computer. But there is antivirus software for cell phone security, just like for computers. You can use that software to protect yourself from viruses. You can also

[3] http://kryptoscommunications.com/
[4] http://www.cellcrypt.com/cellcrypt-mobile
[5] https://whispersystems.org/

protect from viruses by not opening suspicious email attachments and not clicking on sketchy links. You can also make sure to download only trusted apps.

Texting

Text messages are very insecure. They travel through the network unencrypted, are stored on your device, and might be stored for a long time. Text messages are available to just about anyone who gets any access to your phone like corrupt governments, clever hackers, thieves, and unscrupulous competitors. They get it by accessing the network, accessing your provider's records, accessing your phone, and many other ways.

There are some secure text message apps available that encrypt your text messages both in transit and at rest on your device. TextSecure for Android, maintained by **WhisperSystems**,[6] is an open source example.

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

Voicemail

Voicemail is stored by your service provider on their server. Rogue employees, corrupt governments, and hackers are the most likely to have unauthorized access to voicemail information.

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

A small offshore VoIP service is less likely to reveal confidential data than a larger service provider.

Photos

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

[6] https://whispersystems.org/

Turn GPS tracking off. Some phones let you turn off geotagging in the settings. Turning geotagging off can prevent the data from ever being added to the picture file.

Wipe your sensitive data before uploading or emailing.

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

Mobile Apps

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

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

Email

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

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

Web Browsing

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

Your Internet provider can see every website that you visit.

All of this data is readily available to rogue employees and corrupt governments. In many

cases it may be sniffed out by clever hackers and sneaky competitors. Most of this data is also stored right on the phone where anyone that has physical access, even the casually curious, can find it.

You may be able to use anonymous web surfing. Some phones let you use VPNs like the **Tor network**[7] so that your carrier, the web browser, and the websites that you visit can't see where you go on the Internet. The VPN records would only be available to corrupt governments if the VPN is in a cooperative jurisdiction.

SURFING THE WEB

One form of Internet surveillance, traffic analysis, can infer many things over a public network: who is talking to whom and from where. Recording this information can allow others to track your interests and common behavior.

Internet data has two parts, the data payload—whatever information is sent, such as an email or a website—and a header used for routing. Even after encrypting the data, traffic analysis can still record information using the header, which reveals crucial information like location, destination, and the time you sent it.

Even after encrypting the data, traffic analysis can still record information.

To Pay for Proxy or Not

Paying for proxy service can turn your regular web surfing into constant anonymous browsing. Free proxy servers are constantly going online and coming offline. The availability of any one proxy is sometimes limited to days or even hours. Thus, when you find a proxy to use, the chances are that you will have to find a different one the next time you want to surf the web anonymously. If you are anonymously browsing by proxy every time you use the Internet this can become burdensome. Also, many of the free sites whose availability is more reliable will limit your use to a certain number of searches. You will have to rotate between several proxy sites if you want to search more than their allotted minimum.

Paid proxy servers can reduce your time investment for anonymous browsing to a minimum.

In addition, the free software that might allow you to surf anonymously can be difficult to understand and use for the average computer user. Paid proxy servers can reduce your time investment for anonymous browsing to a minimum.

Most paid proxy services are relatively straightforward to use and will be easy to operate for novice computer users.

[7] https://www.torproject.org/

The time commitment will be comparable to what you spend on your antivirus software. Most paid proxy services are relatively straightforward to use and will be easy to operate for novice computer users.

Anonymous Web Surfing Benefits

- **Speed**—Most free proxy servers still want to make some kind of profit. One of the ways they do this is by using advertising. The ads can slow or severely restrict your user experience and make using the free sites cumbersome. Another phenomenon, known as the tragedy of the commons, affects this free resource. The idea behind the tragedy of the commons is that when there is a free resource, the public will have a tendency to overuse it. So the free proxy servers are often overloaded with traffic and therefore run slowly, even if there are no ads. Most of the better paid proxy servers have minimal, if any, advertising and won't noticeably slow down the user experience when using anonymous browsing.

- **Versatility**—Free proxy servers tend to have difficulty displaying some images and many free proxy servers will not give you access to websites that require you to login. Hotmail, Myspace or several other websites are examples. Although there are alternatives which allow you access to most of those sites, many times the free anonymous browsing proxy will only allow access to one of them and you have to change proxies to have access to the others. Most paid proxies will be able to handle any image and allow you access to any page that requires a login.

- **Security**—A computer listed as a free proxy server may itself be a compromised computer. There is even a risk that identity thieves will run a free proxy server and record all of your private data as you enter it. Simply reading up on the server that you intend to use before you use it can help you avoid any problems, but that creates more work for you. I generally do not even use a proxy server unless I can entrust it with my bank privacy. A good, paid, anonymous browsing proxy service will control a network of servers to route your traffic through, making your searching more safe. Paid sites will usually be able to run in the background and protect your computer every time you are connected to the Internet, making the burden on the user minimal.

Anonymous Browsing and Money

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

Free proxy servers are a great way to do anonymous browsing if you have a little bit of time and technical ability. If you have money, or simply lack the time or ability, a paid proxy server can be a great solution. I have a favorite paid proxy server, but there are many to choose from and a different one might better suit your needs.

The potential tax savings from making sure that you are surfing only in tax free states could be tremendous.

USE FREE ENCRYPTION SOFTWARE

Recently, I was scanning information on the latest reported data breaches throughout the United States. A data breach is when personal information, like social security numbers, credit card numbers, etc., that could be used for identity theft has been compromised. **The Identity Theft Resource Center**[8] publishes this figure, along with having a lot of other useful stuff.

The data breaches they report all come from either insecurely transferring files, accidental compromise, insider theft, theft by subcontractors, or even hackers. And the report only contains breaches that were reported in the media. As you scan through this **document**[9] from 2013, you notice some very disturbing things. First, you see a lot of recognizable names that might have some of your data. The next thing you might notice is that a lot of those recognizable names have had significant breaches where thousands, and sometimes millions, of records have been compromised.

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

The low number of companies using encryption software is totally ludicrous. Encryption is incredibly simple to use and there is plenty of free encryption software. VeraCrypt is a free, open source program that provides excellent encryption of data and much better privacy. It is the next generation of the the venerable encryption program TrueCrypt, which is no longer in development. The code has been audited by third parties to verify its integrity and security. If you have never heard of VeraCrypt, any other free encryption software, or encryption at all for that matter, encrypting all of your files will take you a total of about eight minutes.

The low number of companies using encryption software is totally ludicrous. Encryption is incredibly simple to use and there is plenty of free encryption software.

- Go to VeraCrypt's website and download the free encryption software. This will take roughly one minute.
- Go through the tutorial which will walk you through, step by step, how to encrypt and unencrypt files. Make some dummy documents and picture files to practice with. About five minutes.
- Once you are done with the tutorial, encrypt all of your most sensitive files. Two minutes.

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

[8] http://www.idtheftcenter.org/
[9] http://www.idtheftcenter.org/images/breach/ITRC_Breach_Report_2013.pdf
[10] http://truecrypt.org/

You will need to specify the size of the encrypted file before making it.

Now for one of the most disturbing things that I noticed: there are several attorneys and law offices on the list of data breaches. Holy attorney-client privilege, Batman! This can pose some serious problems for attorneys in the near future, if it's not a problem already.

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

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

Why not spend eight minutes to potentially avoid millions of dollars in legal fees and damage awards?

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

Bill Rounds, Esq. & Trace Mayer, JD

Bill Rounds, Esq., is a California attorney and holds a degree in accounting from the University of Utah and a law degree from California Western School of Law. He practices civil litigation, domestic and foreign business entity formation and transactions, criminal defense, and privacy law. He is a strong advocate of personal and financial freedom and civil liberties. He operates **HowToVanish.com** and **BillRoundsJD.com**.

Trace Mayer, JD, author of *The Great Credit Contraction* holds a degree in accounting and a law degree from California Western School of Law and studies the Austrian school of economics. He works as an entrepreneur, investor, journalist, and monetary scientist. He is a strong advocate of the freedom of speech and a member of the Society of Professional Journalists and the San Diego County Bar Association. He has appeared on ABC, NBC, BNN, and radio shows and has presented at many investment conferences throughout the world. He operates **RunToGold.com**, **HowToVanish.com**, and **CreditContraction.com**.