PROTECT YOUR PRIVACY FROM BIG BROTHER'S PRYING EYES!

Larry Edelson

Published By: Weiss Educational Services.
Publication Date: September 2015

Weiss Educational Services
4400 Northcorp Parkway, Palm Beach Gardens, FL 33410
www.weisseducation.com
Client Services: 800-291-8545

Our mission is to empower investors and consumers with unbiased information and guidance to protect their savings, build their wealth, and prosper in good times or bad.

The accuracy of the data used is deemed reliable but not guaranteed. There’s no assurance the past performance of these, or any other recommendation, will be repeated in the future.

Larry Edelson's

Guide To
Digital Privacy

Introduction

I'm going to get right to the heart of the matter: This report is about your privacy. Your digital privacy.

I'm not going to review all the reasons you need to batten down the hatches to protect your privacy. You know the reasons. Plus, I cover them in my *Real Wealth Report* on a regular basis and in my columns in *Money and Markets*.

Suffice it to say right now that if you think President Obama, or any incoming President come 2016, is going to reverse any of the policies that have invaded your privacy, think again.

The eavesdropping will continue. The hunt for your financial assets will continue. And it will get worse.

The government wants to know and track as much of you as possible because very simply put — Washington is bankrupt.

In the months and years ahead it will be seeking to get more and more tax dollars from you, seeking to discover and control directly or indirectly, more and more of your financial assets, and it will want to know everything you are doing.

I don't say this lightly, nor am I an alarmist. The fact of the matter is that Washington realizes that it cannot pay off its mountain of debts to fulfill its IOUs to you in any traditional manner.

It knows the economy will not grow enough to generate the tax revenues needed to ever pay off its debt or make good on its IOUs.

It knows it cannot devalue the dollar enough to inflate away the debt.

And it also knows that it can't renege on the debt or on IOU's such as Social Security or Medicare — or there will be holy hell to pay.

It's not, however, just the government you need to be wary of. Large corporations are also monitoring everything you do.

Some of it is quite innocent, simply devising marketing schemes to get you to buy more of their products.

Other invasions of privacy by large corporations are actually indirectly aiding and abetting Washington's desire to know as much about you as possible.

But the bottom line is this: No matter what, you need to know the best actions to take to secure your digital privacy, now, not later.

And I repeat: The invasions of your privacy are not going to go away.

The cycles of war that I have researched and reported are part and parcel of it.

As the bankrupt governments of the United States and Europe seek more of your wealth, and as geo-political tensions rise all over the world, invasions on your privacy are only going to become worse.

Hence, this guide to your digital privacy, where I cover the basics you should employ to guard your online privacy.

An important disclosure: In this report I recommend certain experts and services of various companies. I do not receive any compensation in any form from any of them. I recommend them simply because I have found them to offer the best advice and/or services in their respective industries.

My personal favorites are bolded, so that you know precisely what I am doing to guard my privacy.

Now, let’s get right to it ...

How to Help Protect Your Privacy from Prying Eyes

Power corrupts and it is corrupting things on a huge scale. So turning away from the problem will not protect us.

There is almost nothing restraining the surveillance state where hundreds of billions of dollars are spent annually on gathering every bit of personal information on every person in the developed world. Secret rulings from secret courts are used as justifications for it, even though primary laws like constitutions and declarations of rights forbid it.

These facts cannot be denied so can we really pretend that the people acquiring this power can be trusted over the rest of us, especially if they are merely government workers.

History has proven that with power comes the abuse of it by those groups that have the majority of it and this is usually the state.

In this report, I will tell you precisely how to secure your personal privacy.

Content Versus Context

Data thieves stealing information are generally looking for two things: Its content and its context.

Content is easily understood such as the text of an email or the transcript of a phone conversation.

However, context is who communicated with whom and how often. So if the data thief knows who you talk to, how often, and for what periods of time, they can know all about you.

Computers, with their immense memory power, are the perfect weapons used to analyze this data as it enables thieves to steal with even more effectiveness.

The Electronic Communications Privacy Act (ECPA) is a law that makes it unlawful to intentionally access stored electronic or wire communication to obtain, alter, or prevent authorized access to such communication.

However, privacy protection under ECPA is minimal and its shortcomings are evident in ECPA codifying the Smith vs. Maryland decision into a statute. Through a subpoena, the government can obtain basic subscriber information and investigators need only affirm that the information sought is relevant to an investigation.

The Patriot Act expanded this authority and police can now obtain “records of session times and durations,” as well as records of “any temporarily assigned network address, making it faster and easier to identify computer users and trace their Internet communications.

Investigators may obtain through a subpoena the “means and source of payment” that a customer uses to pay for an account with a communications provider, “including any credit card or bank account number.”

Amendments to the Patriot Act stipulate that the pen register/trap and trace language of the ECPA applies to cell phones, an Internet user account, or email address, etc.

Warrants are required to obtain the contents of email messages stored online for less than 180 days but this requirement doesn’t apply to already-opened messages, even if the messages are less than 180 days old.

And now you have no chance of privacy for files that you share online via a file sharing service. And if you fail to secure your wireless network, you have no expectation of privacy for your online communications.

The Patriot Act also eliminated the requirement that authorities confirm the target is actually using the device being monitored allowing wiretapping of pay telephones in the expectation that a roving wiretap target might use one of the phones.

Police, for instance, may monitor all PCs in an Internet café or other public connection point in the expectation that the target of a roving wiretap order may use one such PC.

Further, the legal protection the ECPA provides cellular and cordless telephone calls is more illusory than real. Monitoring cellular and cordless conversations is in some cases so easy as to make the wiretap laws unenforceable.

This is particularly true with older analog cellular and cordless phones. While digitally encrypted cordless and cellular phones are difficult for amateurs to monitor, well-known vulnerabilities exist in all common commercial phone encryption schemes.

If an Internet company suffers a security breach that causes you harm, or allows someone access to your data in violation of laws or its own policies, in most cases, it’s not liable for your loss.

Take Google, for instance. Its terms of service state that, “You expressly understand and agree that your use of the services is at your sole risk and that the services are provided ‘as is’ and ‘as available.’” That’s typical.

Companies have pretty much unrestricted use of your electronic data and any information you disclose to them. In the course of your relationship, they will reserve the right to use it in their account records without restriction and to disclose that information to any third party.

Employers can also monitor employees' computer use and telephone conversations, and in most states they will have little expectation of privacy on their employer's computer system.

Although most employers acknowledge to employees that their computer use is subject to monitoring, not all states require such warnings.

And then there's the NSA, the FBI, the CIA and others. All of them can and will hack into your online privacy.

Protecting Your Web Surfing

Web surfing is simply computers communicating with each other via a specific set of protocols.

Since every web transmission contains the address of both sender and destination, intercepting the transmission gives away a lot of very critical information about you, the sender.

That means that whenever you look at any web page on the planet, a record is being created that includes the pages you viewed.

The address of your computer is called an IP address or "Internet Protocol "and is your computer's address. The issue with IP addresses is that Internet providers such as your local phone or cable company keeps records on which IP address belongs to whom.

To translate these numbered IP addresses into a more easily remembered form, a service called DNS is used. Every time you go to a new web site, a DNS system is also involved, and it also grabs your data.

Now that governments and others are massively spying on the Internet (with the seemingly eager assistance of Microsoft, Google, Facebook, Apple, AOL, Yahoo, and many others), you can be sure that every web site you surf is recorded and saved.

Your course of action: In order to avoid surveillance, you must hide your IP address by fixing up your browser program to stop leaking data.

My first recommendation: Stop using any browser EXCEPT Firefox. It's free and is not only a good browser, but it is an open source browser meaning all of its programming is visible so that nothing can be hidden.

Second recommendation: Hide your IP address. That way you are anonymous.

Anonymous networks come in two primary types:

1. TOR (The Onion Router)

2. A VPN (Virtual Private Networks).

TOR

TOR (The Onion Router) is free software that gives you online anonymity by directing Internet traffic through a worldwide volunteer network made up of four thousand internet relays that hide your location.

It's simple to download, install and use. You may download it via this link: www.torproject.org.

TOR will make it difficult to trace Internet activity back to the user and even a top secret appraisal by the National Security Agency has listed TOR as "the King of high secure, low latency Internet anonymity" with "no contenders for the throne in waiting".

Onion routing refers to layers of encryption used to anonymize communication where it encrypts the original data as well as the destination IP address, several times sending it through virtual circuits with successive random TOR relays.

A layer of encryption is decrypted by each relay to reveal yet another relay in the circuit so that it can pass the remaining encrypted data on to it.

The final relay is decrypting the innermost layer of encryption sending the original data to its destination without showing the source IP address.

TOR provides strong anonymity that a hacker won't be able to overcome.

I highly recommend using TOR for the most sensitive web browsing. Use Firefox for normal browsing, TOR for anything you search for on the web that is financially related. Bill paying, shopping, brokerage, trading, etc.

VPN

VPN (Virtual Private Network) is an encrypted connection to a server used by most large companies. In order for a VPN service to be considered usable, it would need encryption and multiple hops.

Some other requirements for VPN to be considered usable is to have its own DNS system so that translation between addresses and website stay private and also that it has out of band authentication, meaning log ins are handled by an external server.

A viable VPN service should not know who is logging in and the time they logged in — a separate server accomplishes this. The network knows only that a user is authenticated (a paying customer), not the details of the user's login.

Lastly, it should NOT have a single point of failure. Meaning customer data and network data should never be in the same place, under the same control so that there is never a single place that can be attacked, giving the attacker enough data to break the user's anonymity.

The only VPN available that meets the criteria mentioned above is Cryptohippie.

I often use Cryptohippie. It's simple to use, and the speed is better than with the other VPNs that I have tested.

You can order and download Cryptohippie via its webpage at secure.cryptohippie.com.

I recommend the company's *Road Warrior* product. Easy to install and use, the software connects you to Cryptohippie' networks and secures your communication via the companies VPN. Cost: $275 but well worth it.

How to Keep Your Emails Private

When you hit send on any email message it is sent to the server of your Internet Service Provider (ISP) and with the way the Internet works, your message might bounce around to many different servers or hops before arriving at the server of the recipient's ISP.

It is on this journey of passing through hops where they can be grabbed and stored by government agencies monitoring the Internet, which can also be made easier by the fact that ISPs are also required to hold copies of messages for a certain amount of time depending on jurisdiction.

Also, data thieves may decide to 'hack' one of the hops stealing your data as it passes along the chain of ISPs.

To prevent this, here are the steps I recommend you consider taking:

Step #1: Secure your email host. First, do not use public mail services like Gmail or Yahoo. These mail services give the wrong impression that it is a secured connection — but the reality is that you have no control over your email.

Assurances of security like the padlock symbol next to the website domain are basically meaningless. And now with governments requesting data from these companies, can you really trust such email hosts?

So the most important step is to control your own email by using a smaller service provider in a jurisdiction you can trust to protect your private communications.

Importantly, while Switzerland's banks have caved in to the IRS, Switzerland still honors the privacy of your online communications and digital storage.

Therefore, I recommend Switzerland as the best place to host your email and digital storage.

There are a couple of servers based there such as JumpShip Services www.jumpshipservices.co/ and Century Media www.centurymedia.co.uk, a British company but its servers are located in Switzerland.

However, the best Swiss-based service I have found and that I use is mykolab.com mykolab.com**.**

The service offers excellent storage options, all data is hosted on Swiss servers, and calendars and mobile email is also offered. You can sign up by going to the above link for mykolab.

The email is very easy to use, the company has a webmail page for your email, and you can also integrate the email with a third-party application such as Mozilla's Thunderbird.

Password security is the next step to limit the risk of someone stealing it and gaining access to your account.

To do this, ensure that the email hosting service you choose uses a security protocol called "SSL/TLS" for both receiving and sending messages. This is a must and if you don't see it, don't use that provider's email service.

Step #2: Choose the right email client. Choosing the right email program or email client is important. If you're using a desktop or laptop, Mozilla's Thunderbird is the way to go as it's free and supports multiple encryption methods that I will discuss shortly. However, there is another big reason: Mozilla is open source.

For complete privacy and security, open source is the way to go as it can't be manipulated by thieves since the code that runs the program is available to anyone who wants it. And with everyone including professional developers looking at the code, suspicious activity would be noticed.

Closed source may be great programs; however, only the company who design them knows what the program does and any backdoors that may exist that would allow hackers into your system. An example of a closed source program is Microsoft Outlook.

I use Thunderbird, with some additional security enhancements, outlined below:

Download Thunderbird from www.mozilla.org/en-US/thunderbird. Once downloaded, follow the simple instructions to set up your email account. Then …

1. Turn off Geolocation by going to Advanced settings and clicking on the Advanced category from the selection of images at the top of the panel. Then select the "General" tab and click on the "Config Editor" button on the bottom right side of the panel. Dismiss the warning and scroll down to geo.enabled and then double-click to change the default value to False.

2. Also set it to "must not load remote content."

3. Disable use of add-ons.

4. Disable allowing delivery notifications.

5. Disable JavaScript.

NOTE: Instructions are applicable for Thunderbird 17.0.7

Step #3: Further secure your email messages. This is done by locking down the messages themselves through encryption so that you offer your public key to anyone who wants it once you set up your account.

When someone wants to send you a message, they can secure the email for you. This way, only you can be the one retrieving the message as you are the only one possessing the private key.

Alternately, if you want to send an encrypted message, you need to get the recipient's public key first to secure the email for them so that only they can pick up the message, because they are the only person who has the private key.

You can download GNU Privacy Guard program for Windows www.gpg4win.org/, it's free but is only for Windows users.

Mac users should refer to GPGTools gpgtools.org/.

For linux users, also consider the GNU Privacy Guard www.gnupg.org/.

Depending on the program you use, you'll also need to configure some settings and get a separate plug-in for your preferred email program.

I have GNU Privacy Guard installed on my computers. However, I only use it for very secure emails I and correspondence that I want to have, such as between myself and my attorney.

Mobile Email Security

Mobile devices tend to trade security for convenience making it tougher to secure. But there are some steps you can take to beef this up:

For android systems, I recommend using K-9 Mail, available for free from the Google Play store.

For iPhone/iPad, use iPGMail.

Cloud Storage

Most of you are probably at the stage where you only wish to remotely store your files. In this case, there is only one cloud-based storage provider that I have found provides secure encrypted storage. It's called Tresorit.

Tresorit is run by a respected firm in the storage business.

I am very impressed with the company's service and **I use Tresorit** for all my digital cloud storage. The interface is very easy to use, offering synchronization and backup, and it also very quick and efficient.

Tresorit offers five gigabytes of storage for free. Uploads and downloads are fully encrypted and everything is hosted largely on Swiss servers.

You can find the company’s website at https://tresorit.com.

The program is very simple to download and has a very simple use interface and help program. Highly recommended.

Lastly, keep in mind that companies providing privacy services online are ever evolving, as are the technologies.

That said, it’s important that whatever service providers you opt to use, always check their websites for important news and/or software updates.

Weiss Educational Services

www.weisseducation.com

This publication does not provide individual, customized investment or trading advice. All information is based upon data whose accuracy is deemed reliable, but not guaranteed. Performance returns cited are derived from our best estimates, but hypothetical as we do not track actual prices of customer purchases and sales. We cannot guarantee the accuracy of third party advertisements or sponsors, and these ads do not necessarily express the viewpoints of Weiss Educational Services or its editors. For more information, see our Terms and Conditions. View our Privacy Policy.