A REPORT FROM SOVEREIGNMAN.COM

DIGITAL PRIVACY

A GUIDE TO GIVING NSA THE FINGER.. WITHOUT THEM EVER NOTICING

A BLACK PAPER

SOVEREIGN MAN

I'm not here to tell you that we are being spied on.

That Facebook is keeping track of you and your friends.

That Google is storing your searches, your locations, your emails, your browsing history. Everything.

That the NSA can listen in on every phone call and read every text message.

Everybody knows that.

They know it. We know it. We know that they track our every move. We know about their social network profiling and enormous data centers they are building all over the country.

As I've said before, from Obama's 'kill switch', to ACTA, SOPA and PIPA, to stasi tactics against people like Kim Dotcom, hardly a month goes by without some major action against Internet users.

But it's what's going on in the background that you should be worried about.

As William Binney, another NSA whistleblower and the agency's former Technical Director, recently told me in the May 2013 edition of our premium service, Sovereign Man: Confidential—

"It was around 2003 when they started putting optical fibers coming into the US through ***Y-connector Narus devices****. Basically these would* ***duplicate the data*** *coming across the Internet—one set of packets would go the normal route,* ***the other set would go to NSA facilities.***

There, ***they collect all the data coming in through fiber optics****, reassemble all the data packets into useable information-- emails, file transfers, etc. and then pass it along for storage.*

That means they are taking all that data off the fiber optic lines at 20 main convergence points in the US, collecting almost all of the Internet traffic passing through the US. ***This gets them pretty much control over the digital world."***

But this is no guide to PRISM or other surveillance programs carried out by governments around the world.

No, this Black Paper is about solutions. And we've intentionally kept this as a short list of actionable solutions. No fluff.

This Black Paper is about how you can reclaim some of your privacy and integrity in a world of Big Brother surveillance; how you and your friends can give all state surveillance and unwarranted consumer profiling the finger...without them ever knowing where you disappeared.

In a perfect world there would not be government agents spying on you. And you'd be able to go about your daily life without worrying about someone reading your emails or text messages.

But we are not living in a perfect world, and thus you can always expect the government to do what they have always done throughout history; they lie, they steal, they kill, they spy, and they always strive for more power and more control.

The bottom line is; when it comes to your freedom of integrity and privacy, the government cannot give it to you.

Because your freedom is not theirs to give.

It belongs to you and you alone.

If you want it back, you must take it for yourself

This Black Paper will help you with that.

These are important steps. Please, share this Black Paper with your friends and family, or **share this link** with your social networks.

Now let's take back your privacy.

To your freedom,

Simon Black
Editor, SovereignMan.com

WHAT YOU'LL LEARN IN THIS BLACK PAPER

Keep It Simple Stupid (KISS)

= *The first rule of protecting your privacy online and offline.*

If a solution or software is too complicated, chances are you won't use it, and what good is it then?

This guide is only about the simple solutions; the software, the services, and the solutions that you actually can use on a daily basis without wanting to pull your hair out.

First of all, in each section you will learn what NOT to do.

Second, You will learn how to surf, email, chat, talk, store data, and buy stuff, securely and privately.

You will learn how to make it quite a bit harder for the NSA to spy on you and map your life.

How These Tools And Services Were Selected

You will notice as you read through this report that most of the tools are open-source. This means that the source code is open for anyone to see and improve the software, and also that it's free to redistribute the software and share it with your friends.

This selection is intentional.

First, because when it's free more people will use it.

And second, because if the source code is available for anyone to view, it's harder, if not impossible, to hide a backdoor in the software that can allow someone to track and log your activities or even gain direct access to your computer.

For example; the source code for ***Skype*** is closed so we don't really know if a backdoor is built in or not. It would not be surprising if there is a backdoor considering how Microsoft, the owner of Skype, bends over backwards for the US government in other matters.

Jitsi on the other hand is another voice call software that we'll cover in the section on encrypted voice calls and it's open-source, so if a backdoor was built in it would quickly be discovered.

But just because something cost money or is not open-source does not mean you should avoid it, it just means you need to take a rational and calculated approach to choosing the tools that best suit your needs.

So let's get started.

Secure Your Social Media Habits

Most of this report is about communicating privately, but as we are living in the age of social media there's another aspect of privacy that you need to consider. That the data you *want* to share with the world can be as dangerous and revealing as the data you want to keep for yourself.

So don't share your whole life on Facebook.

This may apply more to the young people in the audience, but think about it; if you're an average visitor to social media websites and apps such as Facebook, Twitter, Instagram, etc., chances are you share some of the following information:

- Your name
- Your birth date
- What you look like
- Past and present locations where you've lived, worked, gone to school, etc.
- Your future travel plans
- What your lifestyle looks like
- Your interests
- Your political and religious views
- Who your friends are
- Details of family members
- And last but not least, **your location every time you log in**

What more could a government agency ask for?

So when it comes to social media, just think one extra time before you post something online, it can save you trouble years down the road.

Secure Your Browsing

The first step to securing and anonymizing your Internet browsing is to choose a good browser, and let's start with the browser on your computer.

Anonymous Browsing on Laptops

Google and Microsoft are both sharing bed with the NSA, so it does not make much sense to use Google Chrome or Internet Explorer.

Instead, visit the Tor Project and download the Tor Browser Bundle, which is a version of Mozilla Firefox that has been customized to use an anonymous subnetwork which anonymizes your traffic. Here's how it works.

As an example, let's say your in New York City and you visit a website or log into Facebook via the Tor Browswer. Instead of showing your IP address and location (which identifies your specific computer), accessing via the Tor network might show that your traffic is originating from London or Barcelona.

Thus with the Tor Browser Bundle, you do not reveal your location and identity *every time you visit a website*. This is **very** important for online privacy.

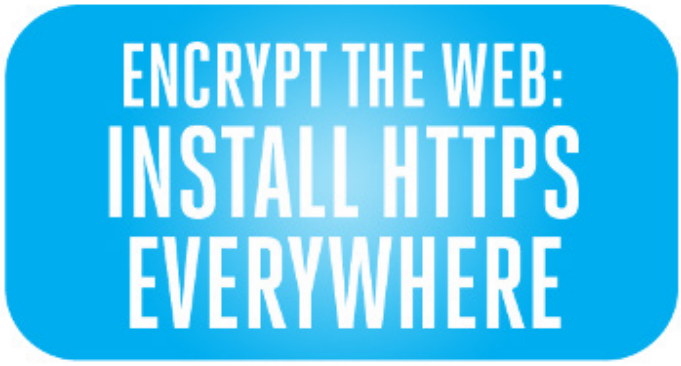
Download the Tor Browser Bundle here, extract the archive, start it up, and you're *almost* ready for browsing the internet more securely.

The #1 Browser Add-On You Should Install

One thing Tor cannot do is **it *cannot* encrypt Internet traffic between the Tor network and its final destination**.

This means that whenever you are communicating information you want to keep safe, for example when you log into a website with a username and password or you log into your online bank, then **make sure you are using HTTPS instead of HTTP**.

A useful (and *free*) plugin that I recommend you install on the Tor Browser is HTTPS Everywhere by the Electronic Frontier Foundation(EFF) and the Tor Project. **This plugin *forces* an https connection** with many major websites and thus encrypts your communications.



But keep in mind when you browse, that "if the browser's lock icon is broken or carries an exclamation mark, you may remain vulnerable to some adversaries that use active attacks or traffic analysis."

Anonymous Browsing on Android

If you've got Android then install the Orbot and Orweb apps. Orbot lets you funnel and encrypt your smart phone traffic through the Tor network and thus makes it anonymous, and Orweb is a web browser that's customized to work with Orbot for anonymous browsing on the go.

Anonymous Browsing on iPhone or iPad

If you use an iPhone or iPad (iOS) device, then check out the Onion Browser ($0.99), which also enables anonymous browsing over the Tor network.

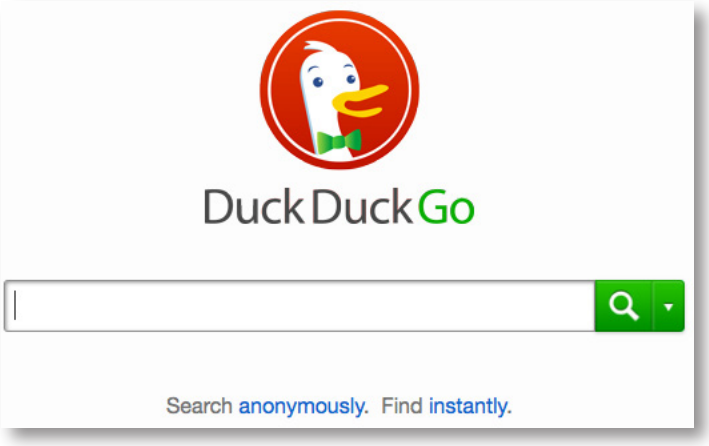
Secure Your Searches (And Drop Off The Tracking Radar)

As you might know, Google stores details about all of your searches-- not only the search term itself but also your location, time and date, etc. (Here's how it works)

They do this so they can *"customize your search experience"* and deliver targeted ads. We also know that they can share all of this data with your government, and they frequently do just that.

The nice thing is there are other search engines out there that will satisfy your search needs just as well, without letting Big Brother peek over your shoulder as you search.

Introducing the search engine for privacy-minded folks: DuckDuckGo.



DuckDuckGo **does not collect or share *any* personal information.** I use it myself, and I can attest that the search results are more than satisfying when compared to Google's search results.

So go and bookmark https://duckduckgo.com, or better yet install their Firefox add-on in your Tor Browser.

Searching on the go?

Get the DuckDuckGo app for iOS or Android.

But...you are not only *actively* tracked when you search on Google or watch videos on Youtube. You are also *passively* tracked when you browse the web through the countless of tracking scripts that you unknowingly run, and cookies that are saved to your computer, when you visit a website.

Google Analytics is just one example, and it's rare to find a website today that does not have Google Analytics tracking set up. This means that you can be tracked on the majority of websites that you visit, and we all know where this data might end up...

The solution?

Block the trackers, so that you stay *invisible* to websites you visit.

To do this, install the browser plugins BetterPrivacy and DoNotTrackMe on the Tor Browser that I recommended earlier in this chapter.

One final add-on to the Tor Browser that you might want to consider is the NoScript plugin, which blocks javascript on the websites you visit. I'll let the creators explain why this may make sense:

"NoScript allows JavaScript, Java and other executable content to run only from trusted domains of your choice, e.g. your home-banking web site, guarding your "trust boundaries" against cross-site scripting attacks (XSS), cross-zone DNS rebinding / CSRF attacks (router hacking), and Clickjacking attempts"

I know that sounds advanced, but if you want to maximize your browser security then you should give NoScript a try and whitelist only the websites that you trust.

Secure Your Email

Whether you have a PC, a Mac, or only a smartphone, you can get started fairly easily with encrypting your emails with state of the art encryption.

But first, let's get one thing out of the way: if you suspect it's a bad idea to use Gmail or Hotmail(now Outlook), you're correct!

Even Hushmail, a company that prides itself with offering "Free Email with Privacy", has been proven to be cooperative with government, as in the cases where they have handed over cleartext copies of private e-mail messages at the request of law enforcement agencies.

They also, as the other big online email services, record your IP address (and thus location) every time you log in to check your email.

So don't use Gmail or any other common cloud based email service for that matter. All of these companies will hand over your data as soon as a government agency knocks on their door.

Now, encryption is all the rage right now, but encryption is only the last step out of three that you need to take to secure your email.

1. Move Your Email Hosting Offshore

First, get your own web domain. If you want to go the whole nine yards then avoid the common .com / .org / .net / .us domains, because they are under the control of the US government, and the US government have a track record of seizing domains they can get their hands on if they think they have a good reason for it.

Domain suffixes such as .no (Norway) or .at (Austria) are run by national-level, non-US agencies that are not under the jurisdiction of the US government.

When you have your own web domain, the next step is to set up your email on an offshore server outside of your native country, and outside of the US. This is not as hard as it sounds, because there are several companies out there offering cheap solutions.

For example NeoMailBox has servers in Switzerland and offers secure email with built in encryption starting at ~$4 per month.

Another alternative that's a bit pricier but more user friendly is the Silent Circle. Their Silent Mail service offers state of the art encryption and comes with your own @silentmail.com email address. Silent Mail is part of the growing Silent Circle suite, and comes from the PGP creator Phil Zimmerman himself.

But remember, using an offshore email provider does not guarantee privacy or security unless you encrypt your emails. But it does decrease the likelihood of your email account being seized by your home government by creating a wall of legal hurdles for anyone who want to gain access to your emails, assuming of course that they try and gain access the legal way.

Because as Henry Kissinger, former US National Security Advisor and Secretary of State, once said: [March 10, 1975 in Ankara, Turkey]

"The illegal we do immediately. The unconstitutional takes a little longer."

So there are two more steps I'd recommend you do that will protect you even if someone would gain full access to your email account.

2. Don't Save Your Emails Forever

Because then what happens if someone gain access to your account? They find years and years of email history. Not smart.

If you use a decent email hosting provider you should be able to configure the email client to delete old emails after a month, year, etc.

3. Encrypt Your Emails

This is the big step. Because if you've encrypted your emails, even if someone gains access to message, all they'll see is gibberish. Don't forget to encrypt your email drafts as well, or better don't save the drafts at all.

The worldwide gold standard for email encryption is Pretty Good Privacy(PGP), or its free cousin Gnu Privacy Guard (GPG). PGP is so good that when it was first invented, the US government considered it a military-grade weapon… and they spent years trying to pin criminal charges on its inventor Phil Zimmerman for violating the Arms Export Control Act.

Encrypted Email for OS X / Windows / Linux

You can configure PGP or GPG to work with most major email clients, including Outlook, Mac Mail, and Mozilla Thunderbird.

The simplest way to get started with encrypting your emails with GnuPGP is to download and install Mozilla Thunderbird along with the Enigmail add-on(check out their Quick Start Guide), along with your offshore email account.

Encrypted Email for Android

If you have a smart phone then unfortunately there are not many user friendly alternatives out there. If you are running Android there's the aging APG (Android Privacy Guard) app that works with the excellent K-9 Mail email app. They're both free, although they do require some proficiency in setting up.

The Guardian Project is hard at work on getting a user friendly GPG app for Android out that makes it easy for everyone to use, and we are keeping our eyes on that project.

Encrypted Email for iOS

Take a look at iPGMail ($1.99), that *"is an app that implements the OpenPGP standard (RFC 4880) and allows the user to create and manage both public and private (RSA and DSA) PGP keys and send and receive PGP encrypted messages."*

Secure Your Chat and Text Messages

In this section you'll learn how to securely chat with and text your friends and family, and we'll cover free solutions for your laptop, your Android smart phone, or your iOS device.

First off, chances are you are currently using the Facebook chat, Skype, Google Talk, Whatsapp, MSN, or regular texting to chat with your friends.

Don't. Because if you do, then the state can read your conversations as an open book.

So let's tighten up your instant messaging security.

First off, if you and your friends happen to have Android smart phones and you text each other, then check out TextSecure.

TextSecure is a free and open source app by Open WhisperSystems that *"encrypts your text messages over the air and on your phone. It's almost identical to the normal text messaging application, and is just as easy to use."*

It will not only encrypt your text messages locally on your phone, but also encrypt them over the air, for full privacy. So if you lose your phone, your text messages will still be protected with full encryption (just make sure you choose a strong password and not 'abc123').

But remember that even though your text messages will be encrypted, your phone company and the NSA will still be able to see that it was you who sent the message, and who received it. So all of that social network profiling will still be going on even though they don't know what you're talking about.

That's why I recommend you use one of the instant messaging solutions below instead. They all use the **Off-the-Record (OTR)** cryptographic protocol, and when combined with Tor no one will be able to know who you are, who you are talking to, or what you're talking about.

The best thing is, with any of the solutions below (except for Cryptocat), the OTR protocol is platform independent, which means you can chat on your iPhone with someone using an Android, PC, or Mac, as long as they also have a client that supports OTR.

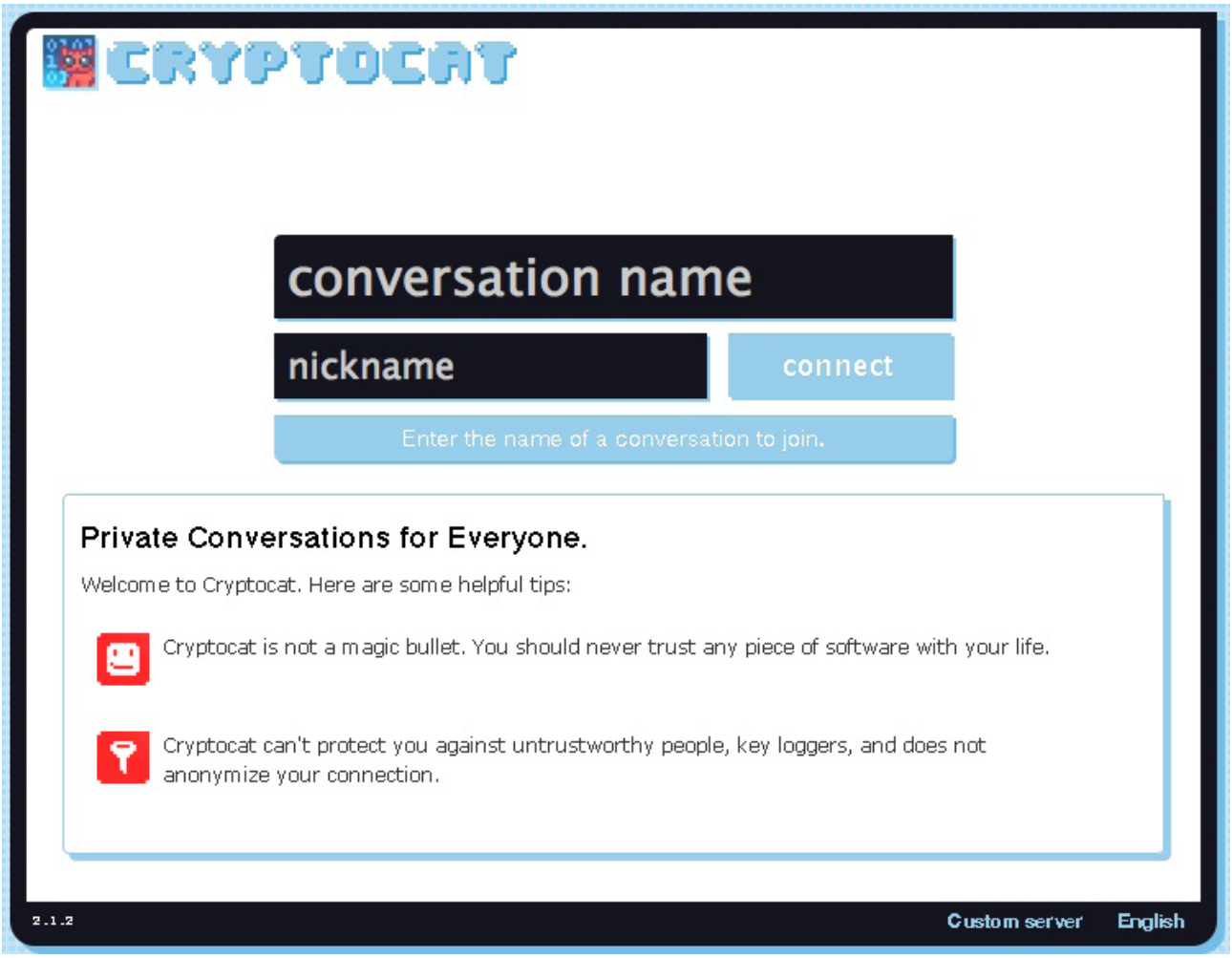
Encrypted Chat for OS X / Windows / Linux

Cryptocat

If you want a really easy solution that just works, then try Cryptocat. It's an easy to use instant messaging client that encrypts your communication with the OTR protocol, and as many other of our recommendations in this Black Paper it's free and open-source.

To get started you can either install the Firefox plugin for your Tor Browser or if you have a Mac you can download the Cryptocat application in the app store.

When you start it up it will look like this:



It's really easy to get started with Cryptocat. Just enter a *conversation name* and a *nick name*, and then click **connect**. To chat with a friend they just have to enter the same conversation name and you will have your own private and encrypted chat room.

As the team behind Cryptocat warns though, this is not a perfect solution:

*"**Cryptocat does not anonymize you:** While your communications are encrypted, your identity can still be traced since Cryptocat does not mask your IP address. For anonymization, we highly recommend using Tor.*

***Cryptocat does not protect against key loggers:** Your messages are encrypted as they go through the wire, but that doesn't mean that your keyboard is necessarily safe. Cryptocat does not protect against hardware or software key loggers which might be snooping on your keyboard strokes and sending them to an undesired third party.*

***Cryptocat does not protect against untrustworthy people:** Parties you're conversing with may still leak your messages without your knowledge. Cryptocat aims to make sure that only the parties you're talking to get your messages, but that doesn't mean these parties are necessarily trustworthy."*

Pidgin / Adium / Jitsi

According to the EFF, "The easiest way to use OTR encryption [on a laptop] is to use Pidgin or Adium for your IMs (Pidgin is a program that will talk to your friends over the MSN, Yahoo!, Google, Jabber, and AIM networks; Adium X is similar program specifically for Mac OS X)."

If you're using Pidgin [the Windows software], install the the OTR encryption plugin for that client. Adium [the Mac software] comes with OTR built in.

With OTR encryption installed, you still need to do a few things for network privacy:

Read and understand OTR encryptions's information

Make sure the people you are talking to also use OTR encryption, and make sure it's active. (In Pidgin, check for OTR:private or OTR:unverified in the bottom right corner.)

Follow OTR encryption's instructions to "Confirm" any person you need to have sensitive conversations with. This reduces the risk of an interloper (including the government with a warrant) being able to trick you into talking to them instead of the person you meant to talk to. Recent versions of OTR encryption allow you to do this just by agreeing on a shared secret word that you both have to type ("what was the name of the friend who introduced us?"). Older versions required that both users check that their client reported the right fingerprint for the other client."

If you'd like to learn more about using Pidgin with OTR then here's a detailed guide that my team dug up.

Jitsi is also a good open-source alternative with OTR support, and as you'll see in the next section you can also use Jitsi for encrypted voice and video calls.

Encrypted Chat for Android

If you have an Android phone and want to chat in private, then the Gibberbot app is what you're looking for. It's open source, it's free, and you can chat with your friends on Google Chat (GChat), Facebook Chat, VKontakte, Yandex, Hyves, Odnoklassniki, StudiVZ, Livejournal, Jabber, etc.

The Guardian Project has a great guide that will get you started with Gibberbot. Check it out here.

Gibberbot also works great with Orbot that we covered in the browser section, which allows you to chat completely anonymous.

Encrypted Chat for iOS

The free ChatSecure app for iPhone and iPad is, just as Gibberbot for Android, an open-source app that use the Off-the-Record protocol for encrypted instant messaging.

Did I mention it's free?

Secure Your Voice Calls

With voice calls let's limit ourselves to VoIP calls, i.e. calls made over the internet, because even if you encrypt calls over the regular cell phone network your telecom provider stores who you talk with, when you talk, and your physical location.

Let's start with what you should **not** be using to make voice calls.

Don't use Skype or Google Voice.

Sure, they do encrypt your voice calls and as Skype states on their homepage; "this protects your communications from falling into the hands of hackers and criminals."

However, they fail to mention if that encryption also protects your communication from falling into the hands of government officials, and will not comment on their rumored backdoor ability to grant law enforcement the privilege of listening in on your calls.

There are more secure alternatives, many of them using the **Open Secure Telephony Network (OSTN)** and the server provided by the Guardian Project, ostel.co**.**

The first step to make encrypted voice calls over OSTN is to sign up for a free account at ostel.co. The username you choose will be the name your friends enter when they want to call you.

Next step is to download one of the clients below depending on your platform and then add your OSTN account, and of course to call a friend over an encrypted line they will also need an ostel.co account and one of the below clients.

When using any of the clients below with OSTN, all the traffic is routed through the Ostel server. This makes is very difficult to track and trace. Not to mention, Ostel doesn't retain any of this data.

Here's instructions from Ostel on how to check if it's working:

"After you install the app on your device, you can test that everything is working by calling the user code named 9-1-9-6. In this echo test, you should hear your own voice when you speak into the phone. You should also see "ZRTP - OK" in the yellow bar near the top of the screen, letting you know that the encryption is working. Now you can place free and secure calls to your friends who also have Ostel set up. To ensure maximum security, confirm that the same 4-digit code appears on both phones."

Encrypted Voice Calls for OS X / Windows / Linux

Jitsi + Ostel.co

The open-source Jitsi app can encrypt your voice and video calls over OSTN. Download the software here and to add your OSTN account, add a **SIP** account to Jitsi with your username@ostel.co email and password.

Encrypted Voice Calls for Android

CSipSimple app + Ostel.co

The CSipSimple app for Android enables you to communicate securely over OSTN. Just download the app in the Google Play store, add your Ostel.co account in their account wizard (with ostel.co as the server name), and then you're all set to call your friends.

RedPhone

An alternative solution for Android is the free RedPhone app by Open WhisperSystems. It's also open source, and has seen real action when it was (and still is) used by dissidents in Egypt during the recent turmoil. Just install it, launch it, and call a friend, and if they have RedPhone installed you will see a notification asking if you want to upgrade to an encrypted call.

One word of caution though: RedPhone only encrypts the traffic between your phone and the other end of the line. As the *Tactical Technology Collective* says *"it becomes easier to analyze the traffic it produces and trace it back to you, through your mobile number. RedPhone uses a central server, which is a point of centralization and thus puts RedPhone in a powerful position (of having control over some of this data)."*

Encrypted Voice Calls for iOS

Groundwire app + Ostel.co

The Groundwire app for iPhone and iPad ($9.99) will allow you to receive encrypted voice calls over OSTN. An additional $25 (in-app purchase) will unlock the ZRTP extension that will allow you to also place secure calls.

Platform Independent Voice Call Encryption

Silent Phone

Silent Phone is part of the *Silent Circle* suite and comes from PGP inventor Phil Zimmerman himself, and have apps for both iOS and Android.

As Silent Circle states on their website "no one can listen in, no one can wiretap." You'll get your own unique 10-digit phone number when you sign up, and the app works over 3G, 4G, or WiFi networks.

As part of the Silent Circle suite you will also find Silent Eyes for Windows that enables encrypted video chat(Mac users, see Jitsi above), and Silent Text (currently only for iOS) .

Secure Your Stored Data

There are many reasons for why you'd want to encrypt your files, photos, or documents.

...on your harddrive

With the open-source software TrueCrypt you can encrypt files containing sensitive information. You can create an encrypted file container or you can encrypt an USB drive, or your entire hard drive.

Download TrueCrypt here, and then check out their beginner's tutorial.

On a Mac, TrueCrypt limits you to creating encrypted file containers, but if you happen to have a Mac running OS X 10.7 or newer you can encrypt the whole hard drive using FileVault, a built in encryption solution.

For a complete guide to FileVault click here.

...in the cloud

We now know that Dropbox has been in the pipeline to be added to NSA's intelligence gathering program PRISM, so it's clear that you should not store sensitive files or documents on Dropbox. Neither can Google Drive, Amazon S3, or iCloud be considered secure places for your data.

You want a cloud storage provider that takes security and privacy seriously and offer strong encryption, and if this is what you're looking for then check out cloud storage provider Mega.co.nz. I'll let the team behind Mega introduce themselves:

"We are a dedicated group of technologists who were given the time, opportunity and Internet access to build an awesome cloud storage service that will help protect your privacy. We have programmed this Internet service from scratch in Auckland, New Zealand. Unlike most of our competitors, we use a state of the art browser based encryption technology where you, not us, control the keys."

The entrepreneur behind Mega, Kim Dotcom, is currently released on bail facing possible extradition to the US in the Megaupload case. If you want to learn what that's all about, then watch this interview with Kim.

To get started with encrypted cloud storage you can sign up for a free account at Mega.co.nz where you get 50GB online storage. If you need more than that you get a lot of bang for your buck with their Pro plans, so drop Dropbox and give Mega a try.

Secure Your Payments

This one is easy.

Whenever possible, **pay in cash**.

By not using your credit card for every purchase you remove yet another source of data that can be tracked and stored indefinitely.

If you can't pay in cash, then consider paying in Bitcoin, if possible.

Bitcoin is a digital currency that is completely decentralized. There is no Bitcoin issuer that regulates its supply like a central bank, and no tiny elite that has the power to conjure new Bitcoins out of thin air.

As such, Bitcoin itself is nearly impossible to regulate, as I noted in a recent article.

Full anonymity requires special efforts though, and here's what you need to know about using Bitcoin.

Download the Bitcoin wallet client here, and to fill up on Bitcoins you can visit Bitstamp.net or Coinbase.com, both of them reputable exchanges.

The Bottom Line & Next Steps

Don't count on government officials, or other bad guys for that matter, to respect your privacy. Their track record proves they don't give a hoot, because for them anything goes in the name of "national security."

Nowadays when you can be a potential terrorist for just about anything, do you really want the state to be able to read you as an open book and store that data forever on a NSA server in the Utah desert?

It might be easy to think that since you're doing nothing 'wrong' then you have nothing to worry about, i.e. the 'nothing to hide, nothing to fear' argument. I'll say it again, it's total BS, because privacy is a right, not a privilege.

Even still, the faux justice system is littered with innocent people who have had their own data wrongfully acquired and used against them.

Our core ethos at Sovereign Man deserves repeating, and it is doing what makes sense no matter what. Taking basic steps to safeguard your communications simply makes sense– no matter what. So start sooner rather than later.

In our free newsletter Notes from the Field I share other strategies that makes sense no matter what, things like:

- opening an offshore bank account in a healthy jurisdiction to protect against insolvent banks
- buying and storing gold and silver offshore to protect your wealth against inflation and corrupt governments
- moving your hard earned retirement savings overseas so insolvent governments can't steal it

- establishing residency in some thriving and exotic country as a backup plan or just to build that better life
- investing in productive farm land that will put money in your pocket when things are going well, and food on your table when the shit hits the fan

If you liked this Black Paper on how to give NSA the finger, then I invite you to join me and over a hundred thousand other men and women as we together explore the future of freedom and prosperity in **Sovereign Man's free newsletter**, *Notes from the Field*.

Click here to sign up for Notes from the Field