

How to Protect Yourself From Big Brother

Contributed by stanklen

Once you've read this article, be sure to read part 2, just released. It delves further, and helps you maintain full anonymity on any computer.

Then purchase a 1 GB USB DemocraKey Kit

You are being watched.

Regardless of the government you live under, your actions on the internet are being tracked. Your every search recorded and kept in a database for future use/abuse. US citizens have had their web traffic monitored by the NSA and AT&T, and their every search history subpoenaed by a Federal Judge. As we move towards a more wired and connected society, the potentials for abuse grow exponentially. Imagine a future where your past searches label you as a threat to your government. Or where your browsing history is known by everyone. It's possible now.

You see, there are fundamental problems with the way the internet was designed in regards to security and privacy. Every email message or web address sent unencrypted (probably every message you've sent unless you're into cryptography) bounces and is routed through open relays around the world, with the potential for snooping at every bounce. The average request for a website bounces through around 12 open relays. That means there are twelve opportunities to monitor your request, without your knowledge.

Clearly, access to information anonymously is the key issue for the future. As countries like China continue to censor the web for information about democracy, and countries like the US continue to monitor their citizen's download history, the average person would seem to have little power to no power to stop the assault on their privacy. Enter encryption.

Encryption has existed for as long as civilization. It provides a proxy layer of protection over every message by making it unreadable without special knowledge. If we're sending e-mail we'll use GPG to make sure no one in between ourselves and our intended recipient can read our message. If the message is intercepted, the most information the person can derive immediately is that they caught a message using GPG. With a few million dollars worth of computers and a team of experts, they may be able to decrypt the message in a few hours, weeks, or months, depending on the key length, but when there are millions of encrypted messages floating around, it's extremely difficult to determine which encrypted message is worth investing the time to decrypt. Thus, your mail is safe. Or safer. For now.

However, when we have millions of people encrypting their every transmission, our chances for privacy go up exponentially, and we have one up on the people who abuse their power. So enough of the chit-chat, let's go about encrypting our every move, and ensuring democracy, free speech, and privacy the world over!

We've got to decide right away what level of paranoia we want to have. If we just want to provide cover traffic for the folks in repressive countries, and don't care about our own privacy, we can get away with just installing a program like Freenet or TOR. Otherwise, we should go about creating our own private environment using my favorite privacy tool, the 1GB USB Key.

By making and using the following USB key setup, you ensure:

- o Your web surfing patterns are much more difficult to monitor
- o Your email is safe from massive snooping
- o Your possession of the software is deniable - even when you give someone the password for your key and your actual key
- o Cover traffic for people and human rights workers in oppressive regimes
- o Freedom of thought everywhere (Hopefully)

Go out and buy yourself a USB key. To anonymize just your web surfing and email, you'll only need a key that's at least 64 MB. If you want to keep hidden files on your key, such as documents, or pictures, you'll need to go as big as you can afford. A 1 gigabyte USB key should be enough for every text file you'd want to transport handily, unless you're also transporting libraries of images or video. In which case, go even bigger.

Download the following files:

TrueCrypt

TorPark
Portable Thunderbird w/ Enigmail & GPG
Portable Gaim (Optional, for Encrypted Instant Messenger)
Portable Abiword (Optional, for creating and editing text files)
Portable GIMP (Optional, for editing and viewing images)

Once we've got all the programs we need downloaded, we can go ahead and create our DemocraKey.

Go first, we'll install TrueCrypt. It can be run off of the USB key in traveler mode, so we can take it with us wherever we go, and be assured of our privacy. Click create volume, and then click create hidden volume. This will guide you through the creation of two volumes, one viewable and one hidden. The hidden one is impossible to prove existing, and thus, the software you will install next won't exist to someone who steals your key!

Next, your going to need to mount the hidden volume. Click mount volume, and be sure to check the protect hidden volume option if you plan on writing to the volume everyone can see. This prevents us from accidentally corrupting our hidden programs or files. TrueCrypt will mount your hidden volume as a drive letter. Install all your portable files you downloaded earlier to the volume. By opening them and pointing them to the mounted drive letter.

Double click TorPark and start surfing. Torpark is Firefox with the TOR anonymizer built into it. This is my personal favorite, and in my opinion, one of the most important open source projects on the net. The onion router places a layer of encryption over every web site visited, then routing it through random computers, thus making your web surfing nearly impossible to track or trace back to your computer. The software is still in the development phase, but it will become more relevant and important as governments and companies continue to try to censor and control the dissemination of information over the net.

The onion router project tries to create a free, anonymous method to access and disseminate any information, regardless of any physical snooping on the internet backbones or by ISP's. It works in the following way:

Keep a look out for this one in helping to get information about democracy behind restrictive, snooping governments. (See: United States, Australia, China, Great Britain, Italy, etc.)Congratulations, you are now surfing anonymously with plausible deniability. You are helping to ensure freedom of speech in countries all around the world and fighting against big brother's snooping.

When you want to send an email, use Portable Thunderbird w/ Enigmail & GPG. Secure and anonymous e-mail has been addressed much earlier than secure and anonymous web browsing. This means the technology for e-mail is more mature, and has been tested a whole lot longer. We know GPG encryption can be relied upon to make sure all of our email transmissions are at least as secure as sealed mail. It works by creating a public key and a private key. You give your public key to anyone you want to write to. They give you their public key, and you encrypt your email with the public key of the person you're talking to. Your email is then only readable by the person you send it to. With plenty of anonymous remailers around to send our email through, we can also be reassured our communication is anonymous. In other words, we can say it's technically impossible to prove an email was sent by us. This is a good thing.

Once you've read this article, be sure to read part 2, just released. It delves further, and helps you maintain full anonymity on any computer.

If this story was useful to you, please spread the word about the need for strong cryptography.

You can discuss also this article and privacy in general further in the forums. If you need help setting up your key, go there.

If you can't get this to work, or you don't understand parts, there are commercial alternatives for those who can't follow these steps. My personal favorite is Anonymizer. Anonymizer provides a similar level of protection in a much easier to use way. I can't recommend it enough for those who aren't able to use the free software above, or have mission critical privacy needs. This software is legal now, but for how long?

UPDATE: Local search engine naplesishome.com has created a site to help out the Open Source volunteers creating

privacy software. Start searching, and every search you make donates a little bit of money to Open Source developers and the Electronic Freedom Foundation (EFF). I recommend setting it as your homepage so contributing is effortless.

UPDATE: You can now purchase DemocraKey kits through Paypal for \$105 with shipping and handling.

Purchase 1 GB USB DemocraKey Kit

A portion of proceeds will be donated to the EFF and to the Open Source Software creators.