Surveillance Self-Defense International

6 Ideas For Those Needing Defensive Technology to Protect Free Speech from Authoritarian Regimes

and

4 Ways the Rest of Us Can Help

By

Peter Eckersley, pde@eff.org

July 2009

ELECTRONIC FRONTIER FOUNDATION
eff.org

Surveillance Self-Defense International

6 Ideas For Those Needing Defensive Technology to Protect Free Speech from Authoritarian Regimes

and

4 Ways the Rest of Us Can Help

Introduction: The Internet remains one of the most powerful means ever created to give voice to repressed people around the world. Unfortunately, new technologies have also given authoritarian regimes new means to identify and retaliate against those who speak out despite censorship and surveillance. Below are six basic ideas for those attempting to speak without falling victim to authoritarian surveillance and censorship, and four ideas for the rest of us who want to help support them.

I. Ideas for Activists and Others Facing Authoritarian Regimes

1. Understand Risk Assessment

The first step in trying to defend yourself against digital surveillance and censorship is to understand the concept of *risk assessment*. Risk assessment is the process of deciding what threats you face, how likely and serious they are, and how to prioritize the steps you can take to protect yourself. EFF's section on risk assessment in Surveillance Self-Defense can help you with this assessment: **https://ssd.eff.org/risk** (Many aspects of the Surveillance Self-Defense website were designed for people living under U.S. law; these may not be applicable in other countries, but the risk assessment prinicples are universal.)

2. Beware of Malware

Malware is a catch-all term for computer viruses, worms, trojan horses, keystroke loggers, spyware, rootkits and any other kind of software that makes a computer spy on you or act against your interests.

If a government is able to install malware on the computer you are using, then it doesn't matter what other steps you take: your files and communications will be subject to surveillance.

If you have your own computer, you need to be sure to install security updates and run antivirus or rootkit scanning software. You also need to understand that these measures only offer

limited protection. For one guide to anti-virus and firewall software, see the Tactical Technology Collective's **"Security in a Box"** guide.

It is important to note that if you are using a shared computer, such as a computer at an Internet cafe or a library, the risk of surveillance by malware may be greater. If you need to use a public computer for sensitive communications, you should use a bootable USB device or CD (such as **Incognito**) to mitigate the risks posed by malware.

You can use a bootable USB or CD for the most sensitive things you do with your own computer, too.

3. Choose the Least-Risky Communications Channels

You should be careful in choosing the channels through which you communicate with other individuals and activists.

a) Talking in person is usually the safest way to speak (unless others are watching you, or your location is bugged).

b) Understand the risk associated with phone calls. Most governments are able to record who calls whom, and when, all of the time. Currently, most governments outside the US/EU have a more limited, albeit unknown ability to record and listen to the phone calls themselves. For instance, it is believed that they will be able to tap phones, but only a limited number (perhaps a few thousand) at any given moment. You should always assume that a call to or from a phone belonging to an activist, or regularly used for activism, may be bugged.

c) Avoid SMS text messages. These pass unencrypted through major telecommunication providers and are easy for a government to harvest and analyze on a massive scale.

d) Protect Internet communications by using encryption[1] and by choosing (preferably offshore) service providers that are trustworthy and unlikely to cooperate with your government.

Here are two channels which are easy to use and which offer some protection:

i. Use the OTR instant messaging plugin. This is easy if you and the people you communicate with can install the Pidgin or Adium X instant messaging programs on your computers. Details on how to do this are available **here**. Disable logging to ensure that if your computer is seized, your communications aren't on it.

ii. Use a webmail provider that supports https encryption. Services like **RiseUp.net** place a premium on their users' privacy. Gmail supports encryption, but you *must* **enable it in your settings** and consider whether you can trust Google not to hand your communications to your government.[2] Make sure that every time you send or receive an email, the page uses https — otherwise, your messages could be intercepted.

There are many other ways to arrange for secure communications, although many require more technical expertise. See **SSD** for further detail with respect to securing email.

e) Encrypted Voice-over-IP is possible, but many VoIP services do not support it. Two exceptions are **ZPhone** and Skype. Unencrypted VoIP is very easy to tap, including most telephone cabinets at Internet cafes.

The level of security afforded by the popular commercial VoIP service Skype is unknown. We believe that countries with sophisticated intelligence services will find ways to defeat Skype's security, while less sophisticated intelligence services may be confounded by it. China is known to have produced its own

trojan-infected version of Skype. It is also known that there are weaknesses in Skype's security architecture.[3] You should assume that the intelligence services of countries like the U.S., Israel or Russia could defeat Skype's encryption. But as far as is known, most less developed countries are unlikely to be able to decrypt Skype's communications in the near future.

4. Use Encryption to Prevent Surveillance and Censorship of your Web Usage

Censorship and surveillance of Internet connections are intimately connected: it is difficult to censor communications without at the same time being able to watch and understand them, because it is difficult for the censorship system to tell the difference between the communications it intends to block and those it does not.

There are many ways to use encryption to protect your communications against surveillance and censorship. You can use some Internet services with their own encryption built-in (see above for instant messaging, or webmail using https). But if you want to use encryption to protect all of your web browsing, try one of the following:

a) Use **Tor**. Tor will encrypt your communications and bounce them around the planet before sending them on to their destination. It offers a high level of protection against eavesdropping by your government[4] and is not hard to use. The greatest challenge with using Tor is that it often slows browsing down a great deal; expect pages to take be slowed down by 10 seconds or more.

If you live in a country where *the very fact that you use Tor* might be seen as grounds for singling you out for arrest, further surveillance, or other unwelcome scrutiny, you should only use Tor in combination with a Tor Bridge. See section 6 below.

b) Use an encrypted proxy or Virtual Private Network (VPN) to tunnel your traffic overseas. This approach offers slightly less protection than Tor but tends to be faster. There are many ways you can try this:

   i) Use a public, SSL-encrypted proxy server. Understand that unless you know who runs a proxy, there is a chance that it is run by your adversary.

   ii) If you have access to a Linux or Unix account overseas, you can instantly create your own encrypted proxy server using the ssh program (which comes installed on Mac OSX and Linux computers, and can be easily installed on Windows). Here are **two pages** discussing how to do that.

   iii) Use a service like **Hotspot Shield**.

   iv) Use an overseas VPN service. Companies such as **Relakks** sell access to services of this sort.

5. Be Careful of What and Where You Publish

a) Avoid publishing material under your own name, or including facts that might be clues to your identity, unless you are willing to take the risk that authorities will target you for reprisals.

b) Avoid publishing material through hosting services that have a commercial presence in your country, or which are likely to cooperate with your country's government. Be aware that some countries have **treaties** which lead them to assist other countries' law enforcement requests.

c) Only publish material through services that use https. *You should see the https prefix in the browser address bar, and an unbroken lock icon in your browser window— not just during login, but the entire time you are using the site.*

Tor Bridges are a more discreet way to connect to the Tor network. Normally, if you use Tor, someone watching the network could observe that your computer was connected to the Tor network.[5] If you use a Tor Bridge instead, it will be much harder to tell that you are using Tor.

If you use Tor and live in a country with a strong tradition of Internet censorship, your government might suddenly start blocking connections to the public Tor network. In that case, you should have a Tor Bridge address ready for use if that happens.

If you live in a country where the mere fact of using Tor might expose you to unwelcome attention or worse, you should never use Tor without configuring it to connect through a bridge.

You can find information about how to configure Tor to use a bridge at:

https://www.torproject.org/bridges

You can find some addresses of Tor bridges at **https://bridges.torproject.org/** , or by sending email to **bridges@torproject.org** with the line "get bridges" by itself in the body of the mail.

II. How Can I Help Others Around the World Escape Surveillance and Censorship?

Perhaps you don't live under an authoritarian regime, but you'd like to help people who do. At the moment, here are our main suggestions:

1. Run a Tor Relay

Donate some of your bandwidth by relaying encrypted traffic between Tor nodes. Follow the instructions linked below, but be sure to disable exiting from your machine, unless you intend to run an exit node (see section 3 below)

http://www.torproject.org/docs/tor-doc-relay.html.en#setup

2. Run a Tor Bridge

Act as a bridge, to help people in countries with extreme Internet censorship and surveillance practices:

https://www.torproject.org/bridges#RunningABridge

If you aren't sure whether you should run a relay or a bridge, read **this**.

3. Consider Running a Tor Exit Node

Unlike running Tor relays and bridges, running a Tor exit node requires significantly more care, organization, and commitment. Tor exit nodes are the machines which pass traffic out of the Tor network and on to its final destination on the Internet.

Exit nodes are vital to the operation of the Tor network. But, unlike the rest of the network, much of

the traffic they carry is unencrypted. Tor exit nodes are the machines that will be fetching websites for dissidents in Iran or Burma to read; they are the machines that will be sending blog posts on behalf of those dissidents; they are the machines that will leave digital logs behind on the websites and servers they visit. But because Tor can be used for any purpose, it is also possible that Tor exit nodes will generate complaints about copyright infringement, web-spamming or other forms of antisocial network activity – and those would be associated with the exit node's IP address.

If you decide to run a Tor exit node, it is important to anticipate the possibility of such complaints, and ensure that you don't get blamed for antisocial things that a few of the hundreds of thousands of Tor users do. You should therefore read the **Tor project's advice on running exit nodes**.

4. Run a Proxy for Friends

If you have friends in a country where Internet censorship is a problem, you could run a private proxy for them. Unfortunately, in order to do this securely, you will need to obtain an SSL certificate for the proxy; this is quite an involved process.

If you run a Unix operating system, understand what shell access is, and trust your friends, you could give them shell accounts to use to create a personal proxy with ssh -D.

1. Encryption uses math to transform a message in a way that makes it unreadable to anyone except those that have a means of decrypting the message. You can protect the security and privacy of your information by encrypting it before sending it over the Internet. If encryption is used properly, the information should only be readable by you and the intended recipient.

2. Google Gmail is a good choice from a computer security perspective: it gives you secure email and instant messaging with other people who use Gmail in https mode. The biggest problem with Gmail is that Google might be compelled by your country's laws to disclose your email to the government. This is especially a risk in Western countries, and any other countries where Google has offices and corporate operations that might subject it to local law. Smaller services like RiseUp.net are exposed to fewer jurisdictions, but you should be mindful that your government might regard the very fact that you use a small, privacy-preserving email service as grounds for suspicion.

3. Problems include: the fact that Skype is typically installed from http:// sites and could readily be tampered with by a third party; the fact that the Skype corporation acts as an authentication and PKI broker, and could itself execute man-in-the-middle attacks; and the fact that remote code execution bugs are periodically found in Skype. For a detailed analysis of Skype's cryptographic design, see **http://www.secdev.org/conf/skype_BHEU06.handout.pdf**.

4. Note that while Tor always prevents eavesdropping by your network, ISP and government, you should be careful sending usernames and passwords over http:// with it, since those have to leave the Tor network and travel to the web server unencrypted. https:// websites are safer in that respect.

5. The signs are that your computer connects to a large number of Internet addresses, all of which are in the public directory of Tor nodes.