New American

Written by C. Mitchell Shaw on October 21, 2014

If You Are Sick of Surveillance, Safeguard Your Systems

Thanks to the Snowden leaks, most people don't need to be convinced that data-mining by government agencies and irresponsible corporations is a real problem that threatens our liberties in the digital age. Fortunately, technology is an equal-opportunity tool. Remember that Snowden was able to keep himself and his communications from prying eyes while making not just one, but a series of revelations to journalists. The technologies he used are used by millions every day. They are easily available and largely free to download. Obviously, addressing all that needs to be done and how to do it is beyond the scope of any one article. This article will give you a good place to begin closing the door on those who would violate your online privacy, but it is up to you to learn more. Do an Internet search for the tools listed here, and you will find a trove of tutorials and YouTube videos to help you along the way. Using these tools may involve an uncomfortable learning curve, but the payoff is worth the effort.

Before addressing those technologies, a look at the nature of "Open-Source" software may be helpful. In simple terms, open-source software is licensed in such a way that its source code is available for anyone to view, audit, modify, and redistribute. Because the open-source community is so large and diverse, the likelihood of anything nefarious being hidden in the code is at or near zero. Another benefit of open-source software is that where vulnerabilities exist, they are more quickly discovered and patched as a community of thousands of people works to solve problems. That is why viruses, which are such a problem for Windows and, to a lesser degree, Mac, are unheard of for Linux.

Linux is a great alternative to Windows for those seeking a more secure and liberty-friendly "Operating System." Because it is open-source, there are many different "flavors" (called distributions) available. Two of the most popular distributions are Ubuntu and Fedora. They can be downloaded for free from www.ubuntu.com and www.getfedora.org/. A fairly complete list of Linux distributions can be found at www.distrowatch.com.

While replacing Windows (or Mac) with Linux is the first step in securing your information, it is by no means sufficient in itself. Encrypting your hard drive should be the next step. Encryption turns the data on your hard drive into an unintelligible string of random characters until the correct password is entered. The protection offered by encrypting your hard drive is only as strong as your password, and though the encryption cannot be broken, a weak password can be broken within minutes using a brute force attack. A good password should be long and include uppercase and lowercase letters, numbers, and symbols. All encryption is not equal, as we now know that many encryption software companies have been pressured by the NSA to provide backdoors. Because of this and the closed-source nature of many of these programs, you should only use open-source encryption. Luckily, most Linux distributions include encryption as part of the installation process.

Now that you have a secure operating system and an encrypted hard drive, it's time to look at the way you use the Internet. Never put anything on the Internet that you would not want to see on the front page of your newspaper. That applies not just to social media, but also to online backup and storage. As the recent hacking and subsequent leaking of intimate celebrity photos stored on Apple's iCloud service demonstrate, once it leaves your hands, it leaves your control. Regardless of the privacy agreements or security promises of these providers, *it is up to you to protect your data*. Besides, most social media and online backup and storage companies are more than willing to cooperate with government snooping. Dropbox recently announced Condoleezza Rice as the newest member of its board. It also keeps backups of files months after you delete them and even after you close your account. One way around this is to encrypt any file you backup or store online. A good tool for this is 7zip, which is available as a free download in most any Linux distribution. Another solution is to switch your online backups to a service that offers "zero knowledge" storage. One such service is SpiderOak, which offers encryption for which only you have the password. They cannot even see your data, not to mention allow anyone else, including government agencies, to see it. If required to turn your data over to a government agency, all they would be able to turn over would be the encrypted files and folders.

E-mail is a very insecure form of communication, as it can be intercepted quite easily. It is like sending a postcard through the mail. Anyone, anywhere along the way that intercepts it can read it. The ultimate solution is to encrypt your e-mail. Open-source GPG e-mail encryption is easily installed and is fairly easy to set up. Once you have it set up and get used to using it, the process is fairly transparent. Soon enough, you will forget you are even doing it, and your e-mail becomes inaccessible to snoopers, government and otherwise. Encourage your friends and family to begin encrypting their e-mails, as well. The more normal it becomes, the more people will do it and the more privacy we will all have.

As far as browsing the Internet, the bare minimum security would be to use a browser such as Firefox, which can be downloaded for free at www.mozilla.org. It is much more secure than Internet Explorer right out of the box, but there are some things you can do to make it even more secure. Download and install the HTTPS Everywhere plugin. This will force a secure connection on all sites that offer it. It is not perfect, but it is the same level of security/encryption used by banking websites. Disable third-party cookies and set up Flash to only run on sites you approve (a process called whitelisting). Flash is notoriously insecure and should only be used with caution.

For the ultimate security while surfing the web, you want to be completely anonymous. For that, there is Tor, which stands for The Onion Router. This service uses layers (like an onion) of security and encryption, routing your Internet traffic through a series of servers (called nodes) and creating a fake IP address at each point along the way. The result is that, when used properly, Tor creates real Internet anonymity. The websites you visit have no idea who you are and you cannot be tracked. This is the method Snowden used to contact *The Guardian* and leak the information on NSA spying. Tor is also available as part of a complete Linux distribution called T.A.I.L.S. (The Amnesic Incognito Live System), which runs only from a disc or usb drive. It leaves no trace of having been used and shuts down immediately if the disc or usb drive is removed.

Mobile devices are becoming easier to secure, as well. For many Android devices there are several after-market versions of Android available for those willing to root their devices. Cyanogenmod is perhaps the most popular and certainly one of the most secure. It is free to download at www.cyanogenmod.org. There are risks to rooting your device, however, and if it is not done correctly, it can make the device unusable. In the security settings of all Android devices there is the option of full encryption. For encrypted phone calls and texts on Android, there are applications available. TextSecure and RedPhone, both by Whisper Systems, are two of the best. Apple has claimed that new iPhones are able to be encrypted in a way that puts total control in the hands of the user. Since their software is closed-source, then believing this claim is a matter of trust, and Apple does not have the best record for being trustworthy. There are applications that claim to provide encrypted calls and texts for iPhone, as well, such as Babel, iCrypter, and CoverMe. Again, it’s a matter of trust as to whether these tools are effective. There is one open-source solution for encrypted calls on iPhones. It is Signal, by Whisper Systems, the developers of TextSecure and RedPhone for Android.

There are many more tools available, but if you use those listed here properly, you will go a long way toward making yourself much harder for the NSA or irresponsible corporations to track and monitor. Unless you are a specific target, the tools outlined here are probably sufficient to shut the door in their faces and regain your privacy and security.