New American

Written by **C. Mitchell Shaw** on May 23, 2023

Published in the June 12, 2023 issue of the New American magazine. Vol. 39, No. 11

Digital Privacy in a World of High-tech Surveillance

Since the internet touches almost every area of our public and private lives, internet privacy is an important guiding principle. With Internet Service Providers, mobile providers, major corporations, and three-letter government agencies capturing our browsing histories, maps, calendars, calls, texts, contacts, and more, people are awakening to the need for protecting their online privacy.

AP images

Wake-up call: Edward Snowden revealed the size and scope of government surveillance in 2013. Since then, millions have taken steps to protect the privacy of their data and communications.

But to solve a problem, the problem must first be acknowledged. The tragedy is that — even 10 years after Edward Snowden's revelations about the scope of digital government surveillance — many still dismiss the problem of digital surveillance, believing they have nothing to hide. And many who *do* recognize the gravity of the problem believe that nothing can be done about it.

The "nothing to hide" fallacy has been answered in these pages already; visit Why Should the Law-abiding Care About Electronic Surveillance? for more perspective.

As to the rationalization that "nothing can be done," nothing could be further from the truth. When Snowden communicated with journalists via secure channels and leaked documents to them of the NSA's illegal surveillance programs, he was able to keep his communications private while maintaining an ongoing dialogue. The technologies he used are still easily available and free to download. And they are used by millions around the globe every day.

This article is intended to give you a good starting place to begin protecting your online privacy, but it is up to you to learn more. Search the internet for the tools and tactics listed below, and you will find a plethora of tutorials and YouTube videos to help you along the way. Learning to use these tools may involve an uncomfortable learning curve, but — again — the payoff is well worth the effort.

Mechanics and Philosophy

The tools and tactics listed below will only work if guided by an underlying philosophy of liberty and privacy — a chain is only as strong as its weakest link. The best operating system protected by the most powerful encryption is worthless if the password is weak. Likewise, if you bare your private life on social media, any other effort to protect your privacy is an exercise in futility.

You should decide what information you are comfortable having public. Private data should never be put on the internet in any form. That includes messaging, online backups, and any other method that sends that private information to — or even *through* — the internet (such as email). The single

exception to this rule would be services that use both end-to-end encryption (making the information unreadable until it is decrypted) and zero-knowledge or zero-access (meaning that not even the provider of the service knows the password to decrypt the data).

Once unencrypted files are out of your hands, they are out of your control.

Of the two broad types of software, open-source and proprietary, open-source is generally safer. 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.

This does not mean that every piece of proprietary software contains "back doors" that call home to three-letter government agencies. But given that the source codes of proprietary software are closely guarded secrets, it is impossible to be certain that such software does not contain back doors. Because of this, this writer recommends using only open-source software whenever possible.

Private conversation: In the wake of the Snowden revelations, privacy-protecting apps using robust encryption have been released to help users guard their communications. For instance, the Signal messaging app — with 20-40 million users worldwide — offers encrypted messages, calls, and video chat. (AP images)

Tools and Tactics

Here are some basic tips for protecting your digital privacy. Any local computer company should be able to help you with any of these steps that are beyond your technical ability. If you elect to use a computer company to help with this, avoid the big-box stores and stay with local mom and pop stores; Geek Squad (as an example) has been known to copy customers' hard drives and search them — without a warrant — for federal agencies.

Encrypt Everything

Encryption uses a key to turn pictures, videos, text, and any other file into an unintelligible string of characters that appear random. While the files are in this state, they are unreadable and are only reassembled into something readable by a key that is activated by the correct passphrase. Guard your encryption passphrases carefully.

Written by **C. Mitchell Shaw** on May 23, 2023

Published in the June 12, 2023 issue of the New American magazine. Vol. 39, No. 11

Since unencrypted information is impossible to secure, this writer recommends encrypting everything you can. This means encrypting data at rest (files and folders that live on a hard drive, USB stick, phone, etc.) and data in motion (text messages, emails, phone calls, and other communications sent from one device to another). Dance like no one is watching, encrypt like everyone is.

First, let's tackle your data at rest. Modern smartphones (iPhone and Android) allow for full-disk encryption that requires a passphrase to access the data on the phone. For your computers, Windows, Mac, and Linux all allow for full-disk encryption as well. However, *only Linux uses open-source encryption*. This writer recommends creating a complete backup of all personal files and folders before encrypting your devices to avoid having your data overwritten by the encryption.

For encrypting data in motion, you will need to look at how you send data. For most users, this will include email, text messages, phone calls, and online storage — including calendars, contacts, and online backups.

Encrypting email used to be a fairly difficult task, but thankfully it is now quite simple. Companies such as ProtonMail and Tutanota offer open-source, end-to-end encrypted email with zero-access standards, so you can be confident that your emails are kept private unless a recipient shares them with someone else.

Text messages can be kept private with Signal, which is available for both iPhone and Android. Texts between Signal users are protected by open-source, end-to-end, zero-access encryption. Edward Snowden says Signal is the messaging app he uses.

While it is illegal to encrypt phone calls, it turns out there are ways around that. The law differentiates communications that go over mobile voice towers from those that use mobile data towers. So Signal encrypts phone calls and video calls as data and sends them over data towers. The result is that you can legally make encrypted phone and video calls using the Signal app on your phone to anyone else who also uses Signal. For a better understanding of the government's "rationale" for making certain encryption illegal, see "Government's All-access Pass to Your Privacy" in the July 18, 2016, print edition of *The New American* — available online here.

Online storage of calendars, contacts, backups, and more can be secured via encrypted services offered by both ProtonMail and Tutanota. Each company offers different services, and users should look carefully at what each offers before making a choice. The good news is that competition fosters excellence and pushes each company to offer more and better services as the competition continues.

Browsing the Web

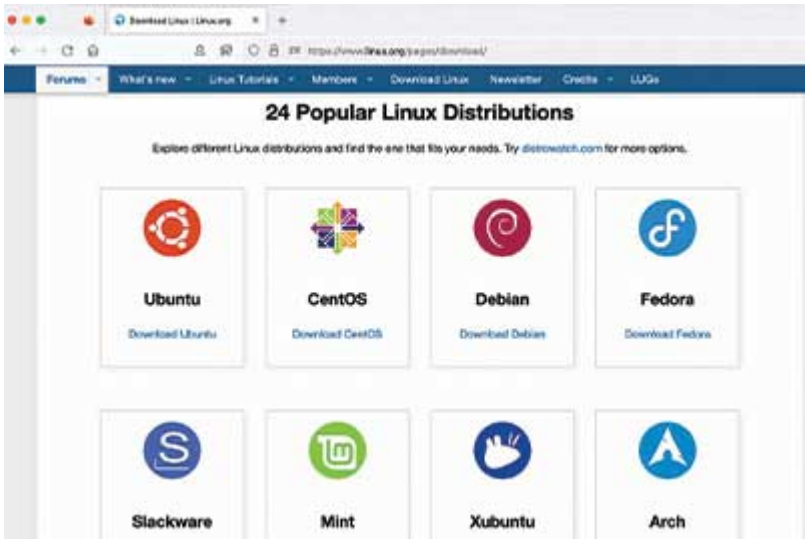
Before addressing how to browse the web with greater privacy, it is important to understand that the "internet" and the "web" are not the same thing. The internet is literally an internetwork — a network made up of networks. Think of it as *hardware,* such ascables, routers, servers, etc. Think of the web as *software* displaying websites on your screen via a web browser, such as Microsoft Edge, Chrome, Firefox, Safari, etc.

Free-market options: Windows and MacOS are not the only choices in operating systems. Linux — which comes in multiple distributions — is a free (as in price and in liberty) and open-source operating system which respects users' freedoms — including privacy. (AP images)

New American

Written by **C. Mitchell Shaw** on May 23, 2023

Published in the June 12, 2023 issue of the New American magazine. Vol. 39, No. 11



Given the very nature of Microsoft and Google, no one concerned about privacy should be using either Edge or Chrome. Firefox is open-source, but it has run into problems in the past few years for caving to the "woke" agenda of the LGBTQ community. This writer recommends the Brave browser. It is a stripped-down version of Chromium (from which Google builds the Chrome browser) with extra privacy protections baked in. It blocks ads that can be used to track users across the web. With all of the code that could be used to spy on users removed, Brave is lean and fast. It is also completely open-source and offers its own search engine — Brave Search — which does not censor or track searches. The search feature is a great alternative to Google (which is an enemy of privacy and liberty).

To secure all traffic to and from your computers and phones, this writer recommends using a trusted VPN, such as ProtonVPN. This encrypts and hides your traffic even from your Internet Service Provider or mobile provider.

Operating Systems

For those who wish to go even further, this writer recommends replacing Windows or MacOS with Linux. Linux is a family of open-source operating systems created in the early 1990s. It differs from proprietary operating systems in some key ways. When a user purchases a computer with either Windows or MacOS, he is not actually purchasing the operating system, but merely a license to use the operating system *in accordance with the End User License Agreement* (EULA) written by the owner (either Microsoft or Apple). With Linux, the user downloads the operating system (usually for free) and *owns* it with full license to use it as he chooses.

Linux is fast, reliable, secure, virus-free, and friendly to both liberty and privacy. While no operating system is perfect, Linux is more secure out of the box than Windows can be made with innumerable tweaks. The two most popular distributions of Linux are Ubuntu and Fedora. Both are free to download and use and are excellent choices. This writer uses PopOS from System76, since it is a leaner, cleaner version of Ubuntu with all of the tweaks that I normally implement with Ubuntu anyway.

Caveat

Neither these tools nor anything else will help you if you are a specific target of a three-letter agency. But these tools should be sufficient to begin protecting privacy for average, law-abiding citizens who want to opt out of mass digital surveillance.

Written by **C. Mitchell Shaw** on May 23, 2023
Published in the June 12, 2023 issue of the New American magazine. Vol. 39, No. 11