Avoiding Internet Surveillance: The Complete Guide

Written by Dann Albright.

Published January 2015.

This manual is the intellectual property of MakeUseOf. It must only be published in its original form. Using parts or republishing altered parts of this guide is prohibited without permission from MakeUseOf.com.

Read more stories like this at MakeUseOf.com
Table of contents

Why Worry About Internet Surveillance? 4
Hide Your Browsing Data 6
Fortify Your Email Security 8
Encrypt Your Chats and IMs 9
Protect Your Messages 10
Secure Your Mobile Device 11
Keeping Your Social Life Private 13
Take Privacy Into Your Own Hands 15
Internet surveillance has been a hot topic in recent years—we’ve talked about it extensively here at MakeUseOf, it’s been brought up on major news outlets daily, and we’ve seen a slew of new apps, extensions, and products aimed at helping you retain your privacy online.

This article is meant to be as comprehensive a resource as possible on avoiding Internet surveillance. We’ll talk about why Internet surveillance is such a big deal, who’s behind it, whether or not you can completely avoid it, and a wide range of tools that will make you harder to track, identify, and spy on.

**Why Worry About Internet Surveillance?**

Before we get into the details of avoiding Internet surveillance, we should discuss exactly what sort of surveillance we’re talking about and why you might want to dodge it. Unless you’ve been living under a rock for a few years, you’ve heard about Edward Snowden and the documents that he released detailing surveillance programs run by the US National Security Administration (NSA) and the UK’s Government Communications Headquarters (GCHQ).


One of the most commonly discussed programs is called PRISM, and it allows the NSA to collect data from the servers of US service providers, including Microsoft, Apple, Google, Facebook, Yahoo!, and others. Anything you have stored on someone’s servers is potentially at risk of being collected and analyzed (to get the details, check out this article on [everything you need to know about PRISM](https://makeuseof.com/tag/what-is-prism/)).

Other programs, like FAIRVIEW and STORMBREW, collect all traffic heading through a specific gateway or router. In both cases, there’s a wide variety of information that could potentially be collected, from *browsing data and history* to emails, chats, videos, photos, and file transfers. There are many others as well, including the recently revealed XKEYSCORE, which could make sure that you’re on the **NSA’s watch list** if you search for privacy-related things like **secure Linux distros** or **virtual private networks (VPNs)**.
Of course, the US and the UK aren’t the only countries collecting data on citizens—it happens all over the world. It just so happens that we know the most about what’s going on in these two countries. And governments aren’t the only ones who are watching your movements online—this information is very valuable to private companies as well. While they won’t be reading your emails, they may track your browsing activity, social networking habits, the apps you use, and information about your friends.

While this information is collected by private companies like social networks and retailers, it’s certainly possible that it will end up in government hands, either through programs like PRISM or through court orders to hand the data over. The same goes for the data collected by your Internet service provider, which you might not even know about (much like users of Telstra had no idea their browsing habits were being logged and sent overseas).

So why might you want to keep governments and companies from getting this sort of information? There could be a wide variety of reasons: you’re a proponent of digital privacy, you’re worried that you could face discrimination or harassment because of your online activity, or because you feel that it violates human rights. All of these are perfectly good reasons for avoiding Internet surveillance.

If you’ve read this far, you’re probably already committed to the idea. However, there are a lot of people out there who believe they don’t have to worry about surveillance because they don’t have anything to hide. If we have a right to privacy, however, this argument is invalid. To find out more
about why this argument just doesn't work, you can read the section on it in my article about the Don’t Spy on Us event.

Now that you have a better understanding of exactly what it is that we’re trying to avoid here, we can get into the details!

Hide Your Browsing Data

More than almost anything else, your browsing habits define you as an online entity. The sites you go to, the ads you see, the links you click—they all create a footprint that’s specific to you and your interests. Even if you don’t use your browser to access disreputable or dangerous sites, concealing this information could be valuable to you, especially if you live in a country that actively suppresses non-standard views (as we’ve seen in Iran, China, and Turkey). So how can you make sure no one’s watching what you’re doing online?

One of the simplest ways to go about concealing your actions on the web is to use a virtual private network, or VPN. When you’re engaging in unsecured browsing, your computer reaches out, through your ISP, across the Internet, to another site. Once you’ve made this connection, you can view that site. However, if anyone is looking closely, they can see that connection. A VPN inserts an intermediary server between you and the site you’re connecting to—if someone is looking now, all they’ll see is a connection from the VPN server to the site on the other end. Your connection to the VPN server is encrypted, concealing your identity.

There are quite a few VPNs that are free, which is great if you don’t use them all the time—many people only use them to access region-blocked video when they want to watch Netflix from another country, for example. If you’re interested in getting a higher bandwidth limit, more speed, and no ads, you should look into paying for a VPN—we have a list of the best VPN services that you can check out. In most cases, it’s as simple as downloading a browser extension or an app, running a five-minute setup, and you’ll be on your way.
If a VPN is thought of as “one hop,” using the Tor network can be thought of as “three hops.” Instead of setting up a single server between you and your destination, using the Tor system bounces your connection through three separate servers before making the connection to the site you want to go to. The increased complexity of the connection makes it extremely difficult for anyone to monitor browsing traffic (though it’s been rumored that the NSA is making some progress in compromising the system).

To use Tor, you just need to download the Tor browser bundle and install it (we have a full guide to Tor available that goes through the process in detail)—then, whenever you use the Tor browser, you’ll be routed through the Tor network. In addition to browsing with significantly increased security, you’ll also have access to .onion sites, websites that can only be visited through the Tor network.

If you want to make sure that your browsing is maximally secure, and that it’s next to impossible to trace, you can route your connection through a VPN and the Tor network. This makes for four servers between you and your destination. No one’s going to go through enough trouble to track you through that mess unless you’re at the top of an intelligence agency’s list.

Another way that your browsing can be tracked is through files that are placed on your computer: cookies. These files can come from a number of sources, but one of the nefarious ways that you can receive trackers is through ads (which, as we have been finding out recently, can deposit a lot of bad stuff on your computer). So how can you prevent these from sending data to snoopers? Ad blocking.

It’s a controversial practice, because ads keep much of the Internet free (see “Are Ad Blocking Browser Extensions Killing The Internet?” and “AdBlock, NoScript, and Ghostery – The Trifecta of Evil”). However, blocking ads will prevent those ads from placing files on your computer. This
means no cookies, no tracking information, and no malware. The prevalence of ad-embedded malware is on the rise, and blocking ads is currently the best way of keeping your computer safe; running an effective antivirus program like Avast is also a good idea (though that might expose you to other forms of tracking, as well).

If you’re not willing to go through the effort (and potentially slow your connection down a bit) to run VPNs or the Tor network on a regular basis, the best thing to do is to download and install a number of browser extensions. HTTPS Everywhere and Disconnect Search are two of the best, and they’re available for both Firefox and Chrome.

Fortify Your Email Security

While browsing creates a digital footprint of your life, email has the potential to carry your most personal secrets, important business communications, and other kinds of sensitive information. While you might not send that sort of thing via email very often, it’s likely that you do discuss your opinions, beliefs, and plans, all of which could potentially be of interest to the government. What can you do to keep your private messages private?

First of all, it’s important to know that securing just one side of an email conversation won’t do you much good. If you send an encrypted message to a friend, and your friend stores it in an unencrypted format on a public server, it’s going to be pretty easy for someone to nab that message. Email is an inherently insecure medium, which means you probably shouldn’t be using it for extremely private things at all. But there are a few things you can do to step up your security.
One of the most well-known and commonly used methods of encrypting email is called Pretty Good Privacy (PGP). The specific mechanics are quite complicated, but you can get the details in this guide to using PGP. In a nutshell, the message is encrypted on your computer, signed with a digital key, and sent to your recipient. That person then uses their own personal key (which is kept secret) to decrypt the message. Theoretically, PGP is nearly uncrackable.

PGP is a very popular option, but setting it up takes some minimal time and effort. If you’d skip the setup, you can use secure services like Hushmail, Vaultlet, and Enigmail, all of which were discussed in this article on secure email providers. These offer a number of different protections that help you rest easy that your mail won’t be easily intercepted and viewed by prying eyes.

Encrypting your mail will go a long way towards keeping the government from reading your messages, but they’re not the only ones who are interested in it. For example, Gmail monitors the contents of your messages for specific triggers that indicate that you might be engaging in specific illegal activities. Earlier this year, the system alerted the authorities to a man who was trading child pornography. In addition to this sort of monitoring, they also scan the contents of your personal messages to better target ads.

Because of the insecurity of email and the fact that your email provider could be scanning your messages, your best bet is to not send anything via email that you’d like to keep private.

Encrypt Your Chats and IMs

We’ve started using instant messages for a lot of things, from quick personal chats to in-depth professional discussions. If you use Google’s chat app, you probably have thousands of IMs saved, and it’s quite likely that if you were to look through them, you’d find a huge variety of things that you don’t want other people to have access to. So what can you do to make sure no one’s snooping on your IMs?

One of the most widely used encryption protocols for instant messaging is called Off-the-Record messaging, or OTR. It uses an interesting style of cryptography called deniable authentication, which means that after the conversation, both participants can deny the existence of the conversation. Using OTR is quite simple: if two people have chat clients that can use the protocol, all they have to do is turn it on. A number of OTR-capable clients are now available, including Adium and Pidgin, which provide OTR encryption for Google Talk, Facebook chat, AIM, Yahoo! Messenger, and a number of other protocols.

In addition to this widely used protocol, there are a number of other less well-known solutions. A great example of this is Cryptocat, a web app that allows you to create an encrypted chat on the fly and invite others to join it by sending a link. After an hour of inactivity, your chats are wiped. It’s one of the easiest ways to encrypt a chat, you don’t need to download anything, and the browser extension lets you fire it up with a click.

SafeChat is another alternative that’s used for encrypting Facebook chats—so if you use Facebook primarily or exclusively for your IMing needs, it’s a good way to go. It’s available not only as a free Chrome and Firefox extension, but also as an iOS app, so you can continue your secure chatting on the go. ChatSecure is another app that allows you to securely use Facebook Chat and Google Talk from your phone.
Remember that with all of these encryption options, like secure email, both parties need to be using encrypted clients, or else anyone who wants to see what’s in your chat can just pull the information from your interlocutor’s computer.

**Protect Your Messages**

Chat, IM, and messaging are all becoming more similar, but there are still times when you want to use an app that’s a bit more like a traditional text messaging app than an instant messenger. Many of the apps that people use on a regular basis from their phones fall into this category, so it’s worth look at on its own. Because almost everyone uses them, they’re of high value to prying eyes—we saw a great example of this in South Korea last year.

There have also been a number of concerns over the privacy of specific messaging clients, such as when Facebook acquired WhatsApp. Although Facebook still hasn’t done much with the messaging app, it’s common knowledge that they collect a huge amount of data on users of their social network (including data on your offline purchases), and there’s been discussion of collecting some of that data through the contents of Facebook chat messages. Obviously, the acquisition of WhatsApp was cause for concern.

Since then, however, WhatsApp has stepped up its game in relation to security and privacy. In a recent Android update, it turned on end-to-end encryption for messages, meaning that not even the servers at WhatsApp contain unencrypted messages. This is a huge victory for privacy advocates. While this encryption hasn’t been enabled for all platforms yet, it’s likely to come in the near future.

Although WhatsApp remains at the top of messaging app popularity list, there are a lot of other great options. Telegram is quickly becoming more popular, and beat WhatsApp to the punch on
many features, like end-to-end encryption, self-destructing messages, and a web client. Telegram’s cloud-based messaging lets you see your messages from your phone, tablet, computer, and any other computer via a browser. The encryption protocol was developed specifically for the app to be highly secure and very fast. And it beats WhatsApp’s great $1-per-year pricing by being free.

We’ve profiled a number of other secure messaging apps in the past, including Silent Text, Threema, Wickr, and Confide. If you can convince everyone that you regularly message to download one of these apps, you’ll have no cause to worry about the security of your messaging. Obviously it’s best if everyone’s using the same app, but the low cost of these options means it’s easy to message one group of friends with one app and another group with another.

Secure Your Mobile Device

While some of the apps and strategies listed above can be used on your mobile phone, there are a few issues that are unique to phones, such as the collection of metadata. If you’ve been paying attention to the latest news on the NSA’s data collection practices, you’ll have heard of metadata—but you might not know what it is. Put succinctly, metadata is information about your information.

Metadata includes things like the phone numbers you’ve called, when you called them, how long you were on the phone, which cell towers you used during the call, and the location of the recipient of the call. Taken together, these things can actually reveal a lot about your conversation and your relationship with the person you’re talking to. Of course, with a court order, government agencies can also easily get a wiretap on your phone, but that’s much less likely to happen.
The difficulty in protecting your metadata is that it’s comprised of information stored by your phone company, and that information can be requested or subpoenaed. Companies aren’t exactly resistant in handing it over.

Unfortunately, the things you can do to protect your metadata are limited. Mobile hardware and software focused on privacy, like the BlackPhone and Silent Circle, helps a lot. They encrypt metadata and make it much more difficult for anyone to obtain it. You can also use a burner phone, if you’d rather not have the NSA collecting data on your phone calls, though this approach does come with some inconvenient drawbacks.

One of the interesting points that a few people have brought up recently is the fact that by offering end-to-end encryption in WhatsApp, Facebook is essentially throwing away a huge amount of potentially valuable data. No one believes that they would offer this feature just for users’ privacy after paying $19 billion for the app, so that value has to be made up somewhere—and most people are pointing to metadata. It’s really valuable.

Beyond the methods above, the best way to keep your metadata out of the hands of the NSA is political: join campaigns to reform metadata-collection laws, hold companies accountable for the data that they hand over to the government, and make sure your voice is heard.

Although it’s tough to prevent the collection of your metadata, there are a number of things you can do to keep the content of your communications private. Using the apps detailed above for messaging is a great place to start (especially if you, like many people, do a lot more messaging than calling). And Guy’s article on three ways to make your smartphone more secure details
Kryptos and Silent Phone, two VoIP apps that encrypt your calls, making them very resistant to any sort of data collection.

Messaging and calling isn’t all that you use your phone for, however—a lot of people also do a great deal of mobile browsing, and just like on your computer, this information can potentially be tracked. To protect your browsing data, there are a number of mobile VPN services that you can set up to use just like the ones discussed above for your computer. We’ve written about HotSpot Shield and VPN Express for iOS, as well as a number of Android VPN apps, that will keep your mobile browsing data safe.

Many VPN services now offer both desktop and mobile protection, and you can get both by signing up for an account—if you’re concerned about your privacy and you don’t wanted limited bandwidth, spending $10 or $15 each month on a premium VPN might be well worth the cost.

Unfortunately, it’s difficult or impossible to prevent your service provider (or Google, or Apple) from tracking your location using the GPS receiver—if you really want to keep anyone from knowing where you are by tracking your phone, your best bet is to turn your phone off and take the battery out, or use the BlackPhone.

And don’t forget to opt out of ad tracking, too. It’s different on each phone, so check out this article on the basics of smartphone privacy.

Keeping Your Social Life Private
Using secure browsing and messaging techniques will keep most of your social networking data from falling into the hands of the government (unless, of course, a social network gives in and hands your data over to the NSA, which is certainly possible). However, social networks—especially Facebook—are doing a lot of surveillance on their own. While they may not be collecting data to see if you’re a potential threat to national security, they can make a lot of money with it. (You can make money selling your own data, too, but that counteracts quite a bit of the advice in this guide.)

The amount of data collected by Facebook is staggering—they collect so much that they can create “shadow profiles” of people who don’t even have Facebook accounts just by collating information from other users’ contacts. Other sites that are linked to Facebook send your information back to their servers (though you can use tools like Facebook Disconnect to prevent that). And let’s not forget about the fact that other companies can gather mass amounts of public Facebook data, too.

While you might feel like your privacy is being violated—even to the degree where it might be illegal in some cases—there’s not much you can do about it. The terms of service of major online services, from Facebook and Twitter to Google and Dropbox, almost always require that you give up at least a good portion of your rights to privacy to use the service. Even your Facebook chats could be scanned.

Even more unnervingly, Facebook can figure out when its ads have influenced your offline purchase decisions. There are very few places where you’re not being surveilled by the social giant. Remember that Facebook isn’t the only culprit here—it’s just the biggest one. Twitter tracks the apps you have on your phone, and we recently published an article on ten social networks that are pretty bad when it comes to privacy.
If you’ve signed up for a social network, they’re almost certainly collecting some data about you. **App.net** is a social network that isn’t funded by ads, so you can probably feel safe that your data, even though some if it’s being collected (as can be seen in their *privacy policy*), won’t be sold to advertisers.

However, you can take steps to limit the amount of data that’s being collected. One of our Facebook Weekly Tips from 2013 dealt specifically with limiting the amount of tracking Facebook can do. You can also opt out of sharing data with Facebook through the Digital Advertising Alliance (though the efficacy of that is debated). It’s a good idea to take these steps, as a lot of social networks, as well as other online companies, may be able to bypass your browser’s security settings.

Unfortunately, the best way to avoid being surveilled by social networks is to not use them . . . and limit the amount of contact that you have with people who do.

**Take Privacy Into Your Own Hands**

As you can see, avoiding Internet surveillance isn’t easy. In fact, completely avoiding it is nearly impossible. And taking all of the steps above will cost you quite a bit of time, effort, and money. But is it worth it? That all depends on how you feel about your privacy.

We know that “nothing to hide, nothing to fear” just isn’t a viable argument when it comes to online privacy. We are being pervasively watched by governments, companies, and service providers around the clock, while we’re on our computers, phones, and tablets. We’re even being watched by social networks when we’re away from our computers—and often when we don’t even have accounts.

As I mentioned earlier, all of this, for the most part, doesn’t really affect our daily lives (other than creating an *information filter bubble*). But if history has shown us anything, it’s that the status quo can be changed at any time, often when we least expect it. And beyond practical safety concerns,
what about our right to privacy? Don’t we have a right to have a private life that’s truly private? That can’t be seen by people who are suspicious of our actions or those who are using us to make copious amounts of money?

It’s time to take your online privacy into your own hands. Use the strategies outlined above and share them with others—the more we fight back against pervasive Internet surveillance, the more likely we are to retain our privacy and online freedom.

Image credits: Beautiful business woman secretly texting (edited) via Shutterstock; Laura Poitras via Wikimedia Commons; Safety concept: pixelated Key, Security concept: Lock on digital screen, Two businessperson shaking hands, Pretty young business woman, Secretive Couple with Smart Phones via Shutterstock; smartphone hand using, View of three nurses in hospital canteen via Shutterstock; Maria Elena via flickr, Projecting The Future via Shutterstock.