what the
GOVERNMENT
doesn’t want you to know

MAKE YOURSELF INVISIBLE TO THE NSA
Make Yourself Invisible to the NSA as Well as All Those Other Snoops, Sneaks & Goons Who Would Simply Love to Plunder Your Privacy!

“But if you have nothing to hide, then you shouldn’t have to worry about the government collecting your metadata.”

Something is very wrong in America when quotes by Nazi German Minister of Propaganda, Josef Goebbels, are used to defend the government’s programs. Goebbels, as you may remember, was one of Hitler’s principal advisers and confidants.

And today, just like in 1930’s Germany, of all the defenses for the National Security Agency’s massive spying program, this one is used most often. The apologists might be Republicans that want to be hard on terrorism. Or Democrats who want to find someway to justify president Obama’s involvement in the program. Or maybe they’re simply your neighbor or coworker who has never been the political type, but goes along with whatever the government says is okay because they just haven’t really thought about it.

People all across the country believe that you need to act like an angel at all times. Failing to do so is your own fault. But let’s examine whether you might have something to fear, even if you believe you’ve done nothing wrong.

As one study showed, there are so many laws on the books in America today, that it’s almost impossible to go through a day without breaking three laws. And that’s only counting federal variety! Once you add state, county, and local laws that could apply to you, the number quickly rises.

And as any police officer will inform you… ignorance of the law is no excuse.

But there’s another important reason why you don’t want the government to keep a record of your emails, texts, phone calls, and other online activity. Even if you never break any laws, the social norms of the present might not be the same of the social norms of the future. And the language you use in your online communications that’s fine today might be inflammatory tomorrow.

The court of public opinion is always open, and the laws that govern that court change as social norms change.

Who knows what you’re saying now that might be construed as offensive or possibly illegal in the future. If you’re willing to believe that your private conversations will remain uncontroversial throughout your life, then you might be able to make the case that the NSA’s surveillance isn’t that bad.

Sometimes you really might not have anything bad to hide. But that doesn’t mean you should be fine handing over the keys to your private life. For most people, they’d rather not have their dirty laundry dug up years later, when times change and what was once the norm is not considered taboo.

The mission of this report is to make sure that doesn’t happen.
The First Thing You Need to Know...

Before we go into how you can make yourself invisible, it’s important to know the inherent limitations of the programs we’re about to discuss. For starters, going invisible and using the right encryption tools can only do part of the job. It’s important to understand the big picture to make sure you protect yourself properly. Your goal is to use tools that help you change your behavior to make it harder for snoops, sneak and other online goons to collect information on you without your permission.

For starters, you need to know that you and the computer you’re using right now has a specific digital fingerprint. The information that’s included in that fingerprint covers a lot of things. From the processor in your computer, to the monitor connected to it.

Individually these things might not be enough to definitely connect you to the computer.

For example, there are many people in the world who are using the same monitor as you. But the number of people who use the same monitor and the same processor is significantly less. Once you add enough variables to the fingerprint (such as the model of your mouse and keyboard, or even the type of browser you commonly use), it makes it very easy to distinguish your computer from all the others on the Internet.

And when you do something on that computer that definitely connects you to it, say order something engraved with your name from Amazon, the metadata stored by the government now has a definitive link between you and your computer.

So with this in mind, it’s important to realize that the advice we’re recommending can only go so far. You might install government level encryption on your mobile phone or device (and one of our recommendations lets you do just that), but if you order a pizza and have it delivered to your house, you’re leaving behind a digital trail.

There’s no magic bullet when it comes to making yourself completely secure, but there are plenty of tools to help you get where want to be. Hopefully, that’s safely outside the watchful eye of Big Brother.

Now let’s begin.

Cryptocat
Online Chats Without the NSA Over Your Shoulder

Twenty years ago, as the Internet started becoming user friendly to the general population, one of the more popular activities was online chatting. Services like America Online and MSN offered users a chance to chat with strangers all around the world about any topic they could imagine. Instead of going down to your local bookstore to talk about the latest novel, you could join an online discussion and share your ideas with a vast new audience.

But somewhere along the line, the powers that be targeted these online discussions. And while posts on messages boards and forums fall under general Internet activity, live active chat discussions eventually
fell under the government’s watchful eye.

Internet messages between two users no longer has the intimacy and privacy of early online interactions. Now they’re stored and mined like other data that passes through cyberspace.

Fortunately, there is a way to gain back that lost privacy. Using an open source program called Cryptocat, users can once again enjoy secure conversations through the Internet. RT America, in fact, has even called the program “kryptonite to the Cyber Intelligence Sharing Protection Act (CISPA).” By denying third parties access to the private conversations taking place via the program, it ultimately makes CISPA irrelevant.

Oddly enough, the fact that it’s open source actually makes your privacy more secure. The nature of the software allows anyone capable of reading computer code to analyze the program. Privacy experts ensure that the programs claims of privacy are legitimate and act as a safeguard for future versions of the software.

While most people in the United States might use Cryptocat to enjoy secure communications without the watchful eye of Big Brother peering overhead, other groups from different countries could use it for a different reason. Protestors around the world know that they’d be at risk if their private messages fell into the wrong hands. If the demonstrators during Arab Spring needed coordinated activities via open networks, the government could easily crack down on them before they could organize.

Like any good technology that threatens to upset the status quo, the government has taken note. The Department of Homeland Security (DHS) detained Nadim Kobeissi, the creator of the program, at the U.S.-Canada border in June 2012. Kobeissi claims that it was the 4th time in the previous three weeks that he was questioned by the DHS. The interrogations usually focused on the Cryptocat’s encryption algorithms, as well as focusing on the creator’s penchant for censorship resistance.

Unfortunately for the DHS, his detainment ultimately increased the popularity of the program. After the owner tweeted about the latest encounter, there was a spike in the number of downloads for the program. The unintended consequence of the government trying to quell online privacy was an increase in the number of people seeking online privacy.

It’s refreshing to find reliable programs created by individuals whose main focus is ideal-oriented. And in this case, the creators of Cryptocat are providing it for free to users.

Find out more about the program from the creators themselves by accessing their website here.

Silent Circle

Untraceable Cell Phone Calls

In our modern world, practically everyone in the country owns a cell phone or some kind of mobile device. It’s a piece of technology that allows us to remain constantly connected to the Internet. And while this has created many more opportunities in our lives, if you’re not careful, it could leave you exposed to online threats.

Twenty years ago, the majority of families only had one phone line in the house. But today’s modern
family might have a different phone number for each family member. And each phone number represents an avenue of risk. Either from NSA software that collects your information, or from potential threats with the technical knowhow to tap your private phone lines.

Regardless of the origin of the threat, there is a practical way to secure your cell phone communications. A relatively new internet startup, Silent Circle, made headlines months ago when they released a mobile app that granted the user government level encryption for all cell phone communications.

The company, located just outside of Washington, D.C., has made it their mission that the government has no business in your personal affairs.

Which is surprising, considering that one of the co-founders, Mike Janke, is a former Navy SEAL. He came up with the idea after trying to figure out a way for him and his fellow SEALs to make secure phone calls back home to their loved ones. After working as a military contractor, he eventually teamed up with Phil Zimmerman, inventor of Pretty Good Privacy (the same encryption software used by NSA whistle-blower Edward Snowden and Guardian newspaper reporter Glenn Greenwald in their initial communications).

The two developed a program that relies partially on a protocol that Zimmerman developed years ago. Silent Circle assumes the role of a service provider. But unlike Verizon, AT&T, and the other major wireless servers, they don’t keep any records of calls made. In fact, the technology that the user installs on their phone actually prohibits Silent Circle from keeping any records whatsoever.

This is the most critical part of the program. And it’s what circumvents the current NSA surveillance network. The system the government has in place copies and stores all metadata that goes across the major carriers systems. So when you make a call on Verizon, both the phone company and the government gain access to that information.

With Silent Circle, however, they prohibit themselves from ever having access to your information. They’ve even said that if they were ever served a subpoena for one of their user’s phone records, they wouldn’t be able to comply even if they wanted to.

As of this writing, the government is not requiring Internet communication programs to be “wiretap-ready.” And in a recent paper, Zimmerman joined with many academics voicing their concern about possible legislation. The owners of this software are putting their money where their mouth is, and creating a system designed with the user’s privacy in mind.

There are other messaging services that offer similar strong encryption software. Surprisingly, iMessages from Apple offers users a high level of protection against outside threats. There is a critical difference, however.

While Apple might keep your messages and information secure, they’ll still store your information. So in the end, they are the ultimate gatekeepers to your privacy. And when Big Government flexes its regulatory muscles, we believe they’ll bow to political pressures than risk upsetting the regulators. Silent Circle, however, does not store your information meaning your security won’t be in the hands of others.

A service as secure as this doesn’t come cheap. It’s a relatively new program, so it’s not surprising
that it costs $20 dollars a month to use it. Check out the website and see if this level of encryption is right for you.

**Tails and Tor**

**Lead the Snoops on a Wild Good Chase Through the Internet**

One of the drawbacks of trying to monitor the entire Internet is that there are a lot of people on it. In the United States, 78.1% of the population has access to the internet. And if you look beyond America, the top 20 countries in the world in terms of Internet users account for roughly two-thirds of the population (about 75% of internet users).

So it’s easy to get lost in the crowd. And getting lost is important if you want to secure your internet activity.

As we mentioned earlier, the government has various programs in place that can track your Internet signatures, and piece together your online identity. When your the telephone number attached to your cell phone account calls your doctor, and then that same phone number calls your child’s school, data mining programs can connect the dots and tie you to that phone number.

But there’s a way to get around that. There is a computer program available on the Internet that allows you to blend in with the crowd, making it more difficult to connect the dots. This may get a little technical, but please bear with us. This could be the most important program you can use to protect your online privacy.

The Amnesnic Incognito Live System (**Tails**) is an operating system that helps mask your online activity. The key component of TAILS is that when multiple people use it, they all leave the same signature behind. Let’s use a quick example to understand it better.

Let’s say you and your neighbor are both fishing enthusiast. You both go to the same sites online to read the latest reviews and articles. If that was the only thing you did on the Internet, when the government records your activity, you’d look exactly the same and there’d be no way to tell you apart.

But let’s say you and your neighbor went to different high schools. When you both check to see how your old alma maters’ are doing, you created another metadata point, and now you’ve differentiated yourself from one another.

But imagine that instead of using two separate computers, you used the same one. So now, you both looked at the same fishing website from the same computer, and then looked up your old high schools. Since you shared the same operating system, there’s no way to differentiate between the two.

Tails is very similar… except instead of just two people using the same operating system, there’s potentially thousands. You see, the program enables users to boot up any computer with a preprogrammed DVD or USB thumb drive. When a computer reboots with the DVD inserted or the thumb drive connected, it loads a specific type of operating system. And it’s the same operating system for everyone who uses the program.

To make your internet activity even more secure, it takes advantage of a virtual system of tunnels
already in place. This system, called Tor, sends your information through a number of different places on the internet. This makes it harder for surveillance software to track and monitor you. It’s similar to those scenes in spy movies where the star of the film takes a windy roundabout way when he thinks he’s being tailed.

Each point in the data’s path has limited knowledge. It only knows the point the information pack just was and the next point it’s going to. So as the information passes along towards its destination, it’s digital trail is practically nonexistent.

When using Tails, all Internet traffic is sent through Tor’s virtual tunnels, protecting you from anyone monitoring your online activity. It’s expanding the idea of using the same computer to a global scale couple with

There are limitations to this program and it’s important to understand them before you use it. This goes back to the earlier discussion about how these security programs can only go so far, and it’s up to you to make sure you stay secure. For example, although your online presence might appear identical to all the other users running Tails, if you purchase something and have it sent to your home address, then you’ve tied your personal identity to that specific activity. The system will still remain intact and you can slip back into relative anonymity with ease, but something as simple as online shopping can expose yourself.

We recommend that you install the program onto a portable thumb drive so you can bring it with you as you travel. Check out the program’s website, and be sure to follow the directions carefully to make sure everything works properly.

DuckDuckGo
Google for the Privacy Minded Individual

Sometimes the best solution to your problem is also the easiest one. We’ve covered a number of programs that you can download that will protect your information. Some are fairly simple, and others more technical. But this next solution is, hands down, the easiest one to implement.

Basically, all it takes is opening up your browser’s settings and changing the default homepage and search engine to a more secure website. Google might be the standard when it comes to finding practically everything on the Internet, but there’s one website that offers similar search capabilities, but you don’t have to trade in your online privacy.

That website is www.duckduckgo.com.

When you first go to the site, you’ll notice right away that it looks very similar to its Google counterpart. And after your first search, the results will seem very similar to Google and other popular websites. But there’s one significant difference.

DuckDuckGo never records any of your personal information or activity.
So while Google regularly tracks your browsing history and uses it to compile a better picture of their users (as well as provide a way for the government to record metadata of users), DuckDuckGo doesn’t store anything. It’s a lot like other privacy and encryption programs that place privacy at the top of their priority risk.

People who understand how this technology works know that they are the gatekeepers to their customer’s privacy. And they’re aware that if their systems become compromised, possibly by online attacks from Uncle Sam, himself, they must hold themselves responsible. And the best way to release them from that responsibility is to remove themselves from the equation.

Besides providing users with a platform to perform searches, DuckDuckGo doesn’t go any deeper than that. In fact, as a result of their refusal to gather personal information of their users, their search results are the same for everyone. As opposed to Google, which customizes results based on a number of factors (such as previous search results and location, just to name a few), DuckDuckGo’s responses depend solely on the terms being searched.

And if the government shows up at DuckDuckGo’s corporate offices demanding to see the search results of you or another American, you can rest easy knowing they’ve hit a dead end.

The real beauty of this solution is that you can use it anywhere at anytime. You don’t have to bring anything with you, and you don’t have to install any software onto the computer you’re using. If you want to stop in at the local library to check look something up, you can use DuckDuckGo and know that your quick search isn’t stored in some government database in Utah. Or that marketers in Google or Yahoo aren’t figuring out the next product to put in your ad sidebar based on your last search query.

Don’t just take our word on it. Check out the website for yourself. Compare it to the search engine that you commonly use and see if it the results are just as good.

Track and Store Every Password You’ll Ever Need

The last solution we have for you is one that we can almost guarantee you’ll use everyday. Though the other solutions we’ve offered keep your information secure from the government, this one will protect you from other nefarious online threats that operate outside the boundaries of the law. More importantly, it will give you the security of knowing the passwords that you use every day are safe and secure.

LastPass is a simple program that acts as a vault for any passwords you use. Using open source encryption software, all passwords are encrypted on your personal computer and can only be accessed via a master password that you control.

An example will better illustrate the benefits of the program. On a given day, you might access multiple accounts to take care of different tasks. You’ll probably sign onto your personal email, maybe buy something off Amazon, and check to see how much money you have in your bank account. It’s possible that if you don’t have your passwords saved, you’ll have to enter three different passwords.
Using LastPass, after you open your browser, you log in via the secure add-on, and all accounts that require a password automatically get logged into. This is especially useful if you’re using a public computer, or one that multiple people use. You might forget to logout of your bank account, leaving it vulnerable to the next person who uses it. But if you log out of LastPass, you can rest easy knowing that all your other accounts are secure.

One of the most significant benefits of the program is that it will take care of generating secure passwords for you. Normally the biggest weakness when using passwords is that there is a tradeoff between user accessibility and password security. You can make a 16 character password consisting of lower and capital case letters, numbers and special symbols, but trying to remember it and enter it correctly every time is extremely tedious. On the other hand, you can make your password simple but then it’s easier for other people to crack it.

LastPass solves this problem in two ways. First, when you create a new account online, you can use the LastPass’ built in tools to generate a unique strong password. Second, any passwords you create with LastPass is saved into your online password vault. You can rest easy knowing that your accounts are secure and not have to worry about memorizing long strings of intricate passwords.

Though it sounds obvious, a program is only as reliable as the people who maintain it. A program that offers the highest level of encryption on the market is useless if the government holds all the important keys needed to access the information. LastPass knows this and takes the necessary steps to protect their customers.

They state on their website that the best way to secure your passwords and online security is to keep your personal information out of their servers. This added level of security not only gives you sole control over your the keys to your online life, but it prevents outside sources like the NSA from tapping into their servers and finding a backdoor to your information.

Like some of the other programs we’ve covered in the report, they understand that the key to reliable security is giving as few people as possible access to your information. This way of operating not only offers you an added layer of protection, but it also protects them from potentially exposing their customers to outside threats.

Click here to check out LastPass’ website and sign up for a free account.

Conclusion

Depending on how much you’re willing to commit, you can get a level of online security that will practically make you invisible to the watchful eyes of the Internet. Obviously, that comes with a cost. And it’s going to be up to you to decide how much is right for you. These are just a handful of option available online, but they’re the ones we feel will give you the best level of security.

If you’d like to continue looking for additional options, we’d recommend taking a look at OpenPGP or Privacy Guard. These will allow you to encrypt the data stored on your harddrives, giving you an added layer of protection.
We’d like to stress one last time that ultimately you, the user, are the most important tool you can use when protecting yourself. You can download all the programs we recommended, but unless you understand and respect their limitations and shortcomings, you could easily expose yourself to the government or other online threats.

Fortunately, with the right setup and a few changes in the way you use the Internet, you can secure your online identity and disappear from the NSA’s crosshairs. Good luck.
Leave the World Alone. It Manages Itself.