How To Avoid The Government Spying On You

Recent events have once again brought to light the fact that the government is spying on us, just as Edward Snowden reported when he left the NSA as a whistleblower.

The two events I'm referring to are the long-awaited Mueller report, which looked into the possibility of collusion between the Trump campaign and the Russians and the arrest of Julian Assange. While Assange's case isn't about government spying, it is about government secrecy and how they hate others knowing what they're up to.

However, I think the really interesting investigation is the one that's about to begin. That is, the investigation into government spying on the Trump campaign, based upon an apparently fraudulent document, paid for by the Clinton campaign.

Click here to get your guide to a layered survival defense!

I think it's important that we understand that the wiretapping of Trump Tower and the Trump campaign headquarters happened while Trump as a private citizen. Granted, he was a high-profile private citizen who was running for president, but he was a private citizen nevertheless. There are laws in place to supposedly restrict the government from spying on private citizens, at least some of which seem to have been subverted to spy on him.

What this seems to mean is that the government doesn't feel itself under any restrictions about spying on US citizens. That viewpoint is supported by a number of Snowden's revelations, especially the ones where he talked about

employees of the NSA sharing interesting personal information they discovered about various people whose electronic communications they had been reading.

Granted, the government probably doesn't have as much interest in spying on you and I, as it did in spying on Donald Trump. That is, unless you are a public figure. But that could change at any time. All it would take is for Trump to lose the 2020 election and the new president to declare that all preppers and survivalists were a threat to the nation. If that were to happen, you could be sure that the investigation would start with the NSA searching their endless database of electronic communications, looking for anyone who has an interest in prepping and survival.

So, with that possibility existing, the question becomes, how do we protect ourselves? It's impossible to cover this fully in an article, but let me hit a few high points.

Social Media

It's amazing the amount of information you can find out about a person from their social media accounts. This is especially true of the younger generation. People post anything and everything about themselves online, sharing their lives with their friends. But no matter what you do with your security settings, you can't keep that information from going beyond your circle of friends. It is also seen by many people you don't know.

Social media has become such a valuable source of information about people, that employers regularly check the social media accounts of prospective employees, to find out more about them. Many a job seeker has probably lost the job they were hoping to get, simply because of things they "liked" on social media, which were interpreted by the company as a black mark against the individual.

Companies aren’t the only ones who do this; the police do to. Many a police investigation has been broken open by what is posted on social media. We’ve all read articles about mass shootings and how the shooter had posted suspicious information on their social media accounts, which was overlooked by the authorities.

Social media companies don’t exist for your convenience, even though they present themselves in that light. Their business is data mining; searching through the mountains of electronic information that they gather about the people who use their platforms and selling that information. Most of the time that information is sold to companies who want it for no more nefarious a reason than to advertise their products to you; but these companies all have a cozy relationship with the government, feeding them information that could have national security or other criminal implications.

Information you put on social media is there forever and is the property of the social media company. Even if you try to delete it, all you accomplish is to hide it from yourself and your friends. It still remains in the company’s database and can still be used for data mining.

The only way to prevent social media from potentially being used against you is to not use social media. Even using it to receive information tells others something about you, as the pages you like indicate your areas of interest. If you follow a few pages about guns and the government institutes a gun ban, you can expect someone to come knocking on your door.

Global Identity Theft Stats

74%
of data breaches were caused by **identity theft**

26%
of total data records breached were **stolen identities**

$16 million
total **identity theft costs** in 2016

Countries with Highest Number of Stolen Identities

UNITED STATES
791,820,040
Major Breaches
FriendFinder

FRANCE
85,312,000
Major Breaches
Dailymotion

RUSSIA
83,500,000
Major Breaches
Mail.ru

CANADA
72,016,746
Major Breaches
Uber

TAIWAN
30,000,000
Major Breaches
Backdoor.Dripion

CHINA
11,344,346
Major Breaches
Suckfly, Buckeye, Tick

SOUTH KOREA
10,343,341
Major Breaches
Internet Explorer

JAPAN
8,301,658
Major Breaches
JTB, Yahoo! Japan

NETHERLANDS
6,595,756
Major Breaches
ransomware

SWEDEN
6,084,276
Major Breaches
Strider

e-Mail

Thanks to Snowden's revelations, we know that the NSA is recording every bit of electronic information on the planet. Actually, that program started back in the 1950s, long before the internet existed. It has grown considerably since then, giving the government a massive database on the lives of every citizen living on the planet.

Somewhere in that massive database is every e-mail you've ever sent. Ask anyone in the intelligence business and they'll tell you that the best source of information is the target person's own words. So, if the government ever really wants to find out about us, all they need to do is call up our e-mails for however many years and read them.

The NSA's echelon program scans every e-mail and other piece of electronic communications, looking for keywords that could indicate terrorist activity or activity by foreign players, aimed at the United States and our allies. Seemingly innocent combinations of words can cause that system to flag a particular e-mail, requiring an analyst, like Snowden, to manually check it. If anything was in the least bit suspicious, they would go back through the individual's e-mail history, looking for anything of potential danger to the country.

I used to quietly chuckle, because my wife didn't want my name attached to any of my writing, especially anything I wrote that was negative towards our government. She was concerned

that I would become a target of some investigation, because I said things that weren't necessary kind about our government and our leaders. She also said the same thing about the survival things I write, thinking that someone in the government might take that to mean that I'm a potential terrorist (rumors of this floated around during the Obama years).

The crazy thing about this is that everything I write is sent out as e-mail attachments. So, even if it doesn't have my name on it, my e-mails have my name on it. Since the NSA has my entire e-mail history in their database, they know what I've written, better than I do. Of course, I never told her that.

… and the Rest of the Internet

Of course, e-mail isn't the only thing that the NSA is tracking; they track everything that goes across the internet. That means they have a more complete history of your internet activity than your computer's history does. Once again, this isn't dangerous to most of us, but if you get flagged by the NSA, what was merely a search born out of curiosity, could end up being a piece of evidence that you are planning a terrorist act.

Let's say, for example that the words backpack and pressure cooker, when together in the same e-mail, are a flag in the echelon program. So some nameless NSA worker starts checking into your history and finds that you searched for how explosives are made. It doesn't matter if that was done for a school project, the combination of the three could lead them to think that you were planning a bombing, leading to a more thorough investigation.

The only way to protect yourself from this sort of scrutiny is to stay off the internet altogether. If you can get an account at your local library or internet café, which does not have your identification or credit card associated with it, you

could probably use it safely; but if they have one piece of data about you, they can piece together your life.

Cell Phones

We don't normally think about it, but modern smartphones are the ultimate tool for spying on you. To start with, your service provider is tracking everything you do over your smartphone, just like the NSA. They're also tracking everywhere you go. Don't believe me? Get on Google Maps sometime and click on "Timeline" in the pull down "hamburger" menu. You'll be able to see everywhere you've been since you had your first GPS enabled smartphone.

There are ways to listen in on your cell phone and to activate the camera remotely. While these are great if you get kidnapped, they're also able to do much more. If the government ever wanted to build a case on you, all they'd have to do is activate that and let you build the case with your own words and actions.

This is why conventional survival defense won't work!

I'm sure you've heard about parents who use online services to track their kids via their smartphones. Those services offer a whole lot more. They also allow you to gain access to the person's entire text message history, their internet history, their call log, the photos stored on their phone and a whole lot more. Smartphones are not private at all, and there are no laws saying that they are required to be. Nor are there any laws yet which restrict law enforcement and other government agencies from using that data.

It's amazing how much of our Fourth Amendment rights we've given up by bringing smartphones into our lives. Totally unawares, we've given others free access into every area of

our lives.

About the only thing we can do to prevent this is to get rid of our smartphones. But we need them, right? The solution is to switch to prepaid burner phones and replace them every once in a while, throwing the old one away. That would be a nuisance and probably look overly melodramatic to our friends, but it would at least give us some modicum of privacy.

Surveillance Cameras

In case you haven't noticed, there are surveillance cameras everywhere. The quality of those cameras has improved too. Whereas surveillance camera footage was blurry and hard to make out a few years ago, the better cameras today are clear enough to make out a face from a block away. This is nothing more than a different application of the same technology that has improved our television's picture.

More and more traffic cameras are being installed, nationwide. At the same time, lower costs are encouraging more and more businesses to install surveillance cameras for security. The lower insurance rates they receive for having a camera make it a logical conclusion for many businesses. Almost all of those cameras are tied into the internet in some way, allowing police and other interested parties to see what's going on.

You've probably seen some cop show where they were following a suspect by camera as they fled the scene of a crime. What you're seeing is a representation of how the police are able to use a combination of government owned cameras and private ones, tapping into and getting a pretty complete picture of what is happening. While there are still areas which don't have camera coverage, they are shrinking day by day.

Avoiding those cameras requires either knowing where they are and what their coverage is, or having some means of defeating them. But neither of those solutions is perfect. Even if you

think you have every camera in an area mapped out, there's nothing to say that you actually have them all. Nor can you be sure of their capability. And if someone adds one, your whole plan goes to pot.

Then there's the problem of blocking the camera. There are means of doing that. One of the easiest is to wear a hat with powerful infrared lights on it. That will wash out the image on the camera, so that they can't see your face. But, since most people don't wear hats like that, simply showing up in front of a camera with one on makes you suspicious. They could track you from a combination of that, your clothing and your stature.

This is a potential problem that's not going to go away. We are gradually becoming more and more of a police state, with the government having more and more capability to spy on us. We are heading for Orwell's 1984, and there's not much we can do about it.