

CHAPTER 9

PERMANENT PRIVACY PROTECTION



THE INTERNET & YOU

Have you ever heard of PRISM? You may not have. It was created with the passage of the Patriot Act, but not officially launched until 2004 when the program officially began. PRISM is a MASSIVE government-sponsored computer operation that enables government servers to capture, catalog and analyze computer transmissions, including but not limited to email, tweets, Facebook posts, and blog comments.

Any and everything you do online can be captured and filed away for later. It doesn't matter if you did anything or not. The government doesn't need a warrant. They do not need to suspect you of anything. They just hook up the equivalent of a giant, digital vacuum cleaner and suck everything up, storing it for review later.

The internet, as people are finding out to their chagrin, is forever. Everything you post online, and every email you send or receive is being captured and spot-checked. There is no such thing as privacy any more. The government is literally the all-seeing eye now, and there is no walking it back.

There is no un-building the machine. Even after the collapse, some remnants of the government will survive to look after the needs of the 1%, and you can bet that agencies like PRISM will be alive and well long after all the services that help the 99% are shut down and relegated to the dustbin of history.

Barely a week goes by that the NSA isn't in the news for some or other infraction. Keep in mind that this isn't some fringe conspiracy theory – this stuff is being reported by the mainstream media, so it is impossible to ignore. Impossible not to take it seriously. Then there are the headlines generated by WikiLeaks and Ed Snowden. These things are happening. They're absolutely undeniable.

PROTECTING YOUR PRIVACY FROM BIG BROTHER

Okay, so you can't provide your own internet access cheaply or easily, but what you CAN do is that when you are online, take steps to maximize your invisibility while online.

There are a couple of excellent ways to go about protecting your anonymity, but one of the best is to download TOR. <https://www.torproject.org/> While nothing is completely untraceable, TOR is about the best security money can buy, and the best part? You do not have to pay a cent. It is an absolutely free, volunteer-driven project. Download and enjoy your newfound web anonymity!

Another excellent option, if you are looking for a way to surf safely, securely, and in (relative) anonymity is to download a browser extension called "Https everywhere." There are versions of this extension for both Chrome and Firefox, so it is easy to find, and free. Basically, this gives you secure socket protection, anywhere you surf.

Bear in mind that neither of these are bullet proof solutions. The government has the resources and the ability to crack the best encryption we can invent. Having said that, the government is like any other thug. If you've got bars on your windows and a top-tier security system, odds are good that they'll pass you by and look for a less well fortified house to rob.

Same thing here. By taking care to protect yourself, you make it unlikely that the government will pry the doors to your defenses unless you give them a compelling reason to do so. They could, sure, but unless they suspect you of something serious, they're not going to go through the trouble, or expend the time and resources that would be necessary. That makes you pretty safe.

WHAT NOT TO DO ONLINE

It is important though, that you ALWAYS be mindful of everything you do when you are online. The normal precautionary rules apply here. Do not go to an untrusted site. Do not enable cookies, or if you have to, make an exceptions list and keep it as short as you possibly can.

Where emails are concerned, again, the usual applies, including do not even OPEN emails that come from people you do not know, and certainly do not click on any links those mails might contain if you DO open them.



There is more though, and here, we need to talk specifically about Yahoo mail. You probably didn't realize this, because honestly, how many people actually READ the Terms of Service when they sign up for a service or account, but Yahoo recently made changes to their terms of service that gives them the right to read ANY of the mail you generate and send from your account.

Their TOS further gives them the right (if you agree to it when you create your account) to access and read the mails of anyone who SENDS mail to you. And they stipulate that it is YOUR responsibility to inform anyone you trade emails about Yahoo's "rights."

Can you believe that? The audacity and nerve it takes a company to ACTUALLY write something like that into a TOS document? The presumption is just unbelievable. Honestly, although Yahoo is the hands-down worst in terms of email, ANY free email service is going to be relatively easier for the government to get their hands on than a paid, secure, encrypted email system.

It may seem pointless to pay for something when you can get it for free, but it all depends on how important your privacy is. Remember the analogy about the thug breaking into homes. If you've got bars on your windows and a big attack dog, and your next door neighbor has the windows open and the doors unlocked, which one is the thug going to break into? Honestly?

You guessed it – they're going to bypass you because you are not worth the trouble. That's why you might want to at least consider using a paid email service. They do not cost a lot, and they're a great deal more secure than the free services.

OFFSHORING YOUR WEBSITE

If you have a web-based business, or heck, even if you do not and you just do some blogging now and then, you should SERIOUSLY consider moving your website offshore. The more revenue your site brings in, the more important this becomes, and the reasons for this are the same as the reasons for creating an offshore corporation and moving your banking out of the country.

The sad truth is that the government can, pretty much on a whim, reach out and shut down any business operating on US shores. You can protect yourself simply by having your site hosted elsewhere. If you are interested in doing that, then the best place to consider is Sealand.

What? You've never heard of The Principality of Sealand? It is its own country. Seriously. The smallest nation on the planet – all of six acres in size, with a population of just 27. The “nation” was started by a quirky family of pioneers, and it has a surprisingly colorful history, including participation in one “war” and diplomatic recognition by a few countries.



The “nation” began life as an offshore platform in the North Sea, in international waters. When it was abandoned, a family moved into it, staked a claim, and then declared it a sovereign state. You can read more about the micronation here: <http://www.damninteresting.com/the-history-of-sealand/>

Of particular interest is the formation of HavenCo, a hosting and data security company based in Sealand, which offers world class privacy and security, and, being that the place is its own, independent “nation” and doesn't have any extradition or other treaties with the United States, it is about as secure a place as you can find to park your website. Find out more about HavenCo here: <https://www.havenco.com/>

<http://www.sealandgov.org/sealand-news-1/HavenCo>

Here are some other options to consider:

- Iceland (<https://www.orangewebsite.com/>)
- Norway (https://hostripples.com/norway_web_hosting.php)
- The Netherlands (<https://www.altushost.com/netherlands-web-hosting/>)
- Romania (<http://www.site5.com/p/bucharest-romania-web-hosting/>)
- Switzerland (<https://www.hostpoint.ch/en/webhosting/webhosting.html>)

Of these, four of them are on the list for their extremely potent privacy laws (now you know why the Pirate Bay has made its home in Norway for about half of forever!), and the last, Romania, because of the connection speeds.

Shockingly, tiny, backwater Romania has some of the fastest internet speeds on the planet! There are, of course, a number of hosting companies in each of these locations. We've included one from each country to get you started, but by all means, supplement this with your own research – you might find an even better deal out there!

The bottom line though, is that if you make any money at all online, you need to get your website OUT of the United States for all the same reasons you moved your bank account and the ownership of your assets. If you do not...if you overlook this point, you might find yourself losing control of a very important income stream. Do not let that happen to you.