Ten ways you can avoid being caught in the PRISM net

Last weekend, the Washington Post published a further four slides, leaked from the US National Security Agency (NSA), which outline how data is collected through the PRISM program.

The process is fairly simple: after an NSA analyst identifies a new surveillance target and a supervisor endorses the analyst’s “reasonable belief” (defined as 51% confidence) that the target is a foreign national and overseas at the time, data collection can begin.

Just say you’re one of these new targets, or you simply don’t want to be incidentally monitored. How can you minimise the amount of data you share?

PRISM’s data collection methods

Commentators generally agree the NSA’s PRISM technology is based on optical fibre “wiretaps” placed at the connection of internet providers to companies like Google, Yahoo and Facebook in the US. (Tapping the signal here gives the companies plausible deniability, as the tap occurs outside their premises - or maybe they just don’t know, as they claim.)

A PRISM slide showing collection dataflow. Wikimedia Commons

A copy of the optical signal is split off and routed to a room operated by the NSA, where it is indexed, categorised and shipped back to the NSA for analysis later. Most of the traffic on the optical fibre is transmitted using plain text protocols – packets which contain a plain text header (to and from address) and a payload (the message).

If the payload is encrypted, the NSA still have a good chance of decrypting it. The NSA spent US$2 billion on a massive data centre in Utah, which is set to open later this year, and have recently commissioned a second in Maryland. These could house enough computers to store the NSA’s collection of intercepted traffic for years to come. Future developments in decryption could allow the NSA to decrypt the messages they are intercepting today.

Under the Patriot Act, which was signed into law in 2001 in response to the 9/11 terrorist attacks, US agencies have the authority to compel companies like Google, Yahoo and Apple to provide their private cryptographic keys to the NSA, allowing the NSA to decrypt secure traffic going through those companies. Under the same act it is an offense to tell anyone it has happened. Even without the keys, some “secure” web traffic can be decrypted using brute force methods.

A PRISM slide showing how targets are identified. Wikimedia Commons

So here are 10 simple ways you can minimise the likelihood of the NSA (and other organisations) monitoring your internet and voice traffic.

1. Encrypt your internet traffic

In the URL field of the browser, type in “https://” before the domain name. Your browser will download a certificate from the website and use it to exchange a shared encryption key. From then on, all your traffic is encrypted. If you don’t see “https” in the URL field, it’s not encrypted.

2. Check the encryption used by the websites you visit

Not all websites use good keys or encryption algorithms. At sslabs.com you can test the sites you visit and (politely) ask them to improve their security.
3. Disable internet use tracking

There are two possible approaches to preventing website tracking: black listing and white listing. Black list programs use lists of known spyware sites and block those activities. PeerBlock is one such program.

NoScript is a white list system, and turns off JavaScript (a programming language which runs in your browser) when you visit a site unless the site is on the list. Most tracking uses JavaScript, so turning it off makes it harder (but not impossible) for the spies to track you.

4. Encrypt your files

If you upload files to the internet, you might want to control who reads them. An easy solution is to password protect them. Microsoft Office products provide the option of setting a password, but this is not particularly strong. Another approach is to put the file in a zip, rar or 7z container and set the password. The best approach is to use a serious encryption system which really scrambles the file contents with a really big key and a strong algorithm, such as TrueCrypt.

5. Trust no-one

Do you use Dropbox? iCloud? Other cloud services? Do you have a password? If you do, so do they. If you forget your password, can they tell you what it is? Some cloud services offer accelerated uploads and syncing. They can do this because they know what you’ve uploaded, and it also means they have the key and can provide it to the NSA. The only way to be sure is to encrypt your files before they leave your computer. Don't use the provider’s encryption software. Use open source software, so any hidden back doors will be discovered. AxCrypt is a nice example.

6. Tunnel your traffic

Pensiero

Every message (or web request) you send on the internet has headers – with your address, the destination address, the date and time. Spooks can use this meta-data to link you to your friends and their friends.

Anonymising services and products attempt to obscure your web behaviour by mixing your traffic with other people’s traffic and by "tunnelling" (encrypting) your traffic between locations. You install a proxy server or a virtual private network (VPN) client, which encrypts your traffic and sends it to another location, where it is decrypted.

The NSA can read the traffic once it leaves the tunnel, but can’t separate your traffic from the traffic of other users of the system. The more users there are, the more anonymous your traffic becomes.

7. Secure your kit

To be sure your PC is free of all unwanted software, you can use a read-only operating system. There are many bootable Linux distributions which detect your hardware at boot time and contain a suite of pre-installed programs such as web browsers and VPN clients. Puppy Linux (really fast) and Privatix (really secure) are good examples. They reveal nothing about your computer and cannot be infected because they don’t write to the hard disk. These are ideal if you’re really paranoid.

8. Safe text

Texting with a phone is not secure. Skype chat is monitored by Microsoft. Email normally uses unencrypted protocols, and is not secure. Even sending emails through websites (with “https”) is no guarantee of security because most mail servers communicate with each other using plain text protocols containing the message, sender and recipient. It is possible to install Pretty Good Privacy (PGP) – an “uncrackable” email encryption scheme - but the process is difficult at best.
However, there are some solutions. Gateway devices can implement PGP at the edge of your network, allowing you to exchange encrypted email with minimal configuration. Phone apps such as Silent Circle and iChat can be used to encrypt text messages. CryptoCat does a similar thing through the web.

9. Anonymous searches

We all know Google caches our search terms and profiles us based on what we look up - it’s how they generate revenue. But there are other search engines which are less interested in what we are doing. Duckduckgo and Startpage are examples of alternatives. Another option is to use a different Google (such as google.de or google.ca), or use [Tor](http://en.wikipedia.org/wiki/Tor_(anonymity_network%29) (anonymity software) or a VPN to use Google from a different country.

10. Voice

Smartphones are great, but they are really little computers, and are vulnerable to malware, phishing scams and a range of malicious phone apps. Skype voice encryption has been weakened by Microsoft to allow lawful interception. Probably the best option for voice security is the BlackBerry – provided you are not in a country where the government has compelled Research In Motion (the company behind BlackBerry) to install a local server so the local police can intercept calls.

… and finally

None of these suggestions can protect you from a really determined adversary, but they can make things more difficult. If the NSA really suspects you, they can always get a warrant and search your house the old fashioned way.

Keep in mind, if you do successfully frustrate them (or law enforcement officers in other countries) there are laws which require you to reveal the passwords or keys used to hide potential evidence, and disobeying these laws can result in prison sentences of at least two years depending on the jurisdiction.