Reset the net

by Tom Shone

June 5th marks the start of the “Reset the net” campaign, a social movement focused on the reclamation of online privacy. The date marks the one year anniversary of the first of a series of revelations by Edward Snowden which detailed just how pervasive mass surveillance is. To mark this event, a number of civil liberties organisations, political groups, and media websites including the EFF, Amnesty International, ACLU, reddit and Greenpeace have banded together to encourage people to disrupt mass surveillance by making it difficult for companies and governments to easily collect our personal information en-mass.

Mass surveillance only works because it is very easy to monitor our online activity. We post mountains of personal details about ourselves online. We use the same password on different websites. We send emails and instant messages over a variety of systems without any idea of who might be listening. As far as governments are concerned, we are standing on the tops of buildings shouting out everything we're doing online to the entire world to hear.

Secure communication

To understand secure communication, you need to understand three simple rules.

- Are you sure that no one can overhear what you're saying to your friend?
- Are you sure you're talking to your friend, and not someone disguised as your friend?
- Are you sure your friend isn't going to tell someone else what you told him/her?

To make sure that we don't fall foul of rule 1, we need to make sure that all our communications are encrypted. If you're using a website, then you should check that your URL starts with https://. To make this a breeze, the friendly team from the Electronic Frontier Foundation put together a helpful plugin for your browser called HTTP Everywhere (https://www.eff.org/https-everywhere). If you're using a chat program, then you should make sure it offers encryption. If you're sending emails, then you need to make sure your settings are configured for secure transfer.

Rule 2 is a bit more complicated and involves ensuring that the SSL certificate of the website you're visiting is signed by a credible authority. It's a complicated way of saying I trust person A, so if person A vouchers for person B, I know I can trust person B. Companies like Thwate and Verisign make their money by being that person A. They mathematically sign SSL certificates to vouch for them. When you visit a website and you get a warning about the SSL certificate being self-signed or the issuer is unknown, this means that either no person A has signed the certificate or you don't trust person A.

For rule 3, you're on your own. You need to decide whether you trust the website you're visiting not to give your personal information away. We already know that almost all the big websites have either handed your personal information over to advertising and marketing third parties, or have been ordered by governments to hand over the information about their users. For the last two years the FBI has been pushing for laws to require all major websites to provide them with an easy-to-use backdoor (http://www.cnet.com/news/fbi-we-need-wiretap-ready-web-sites-now/). The best approach I suggest reducing the amount of personal information you post on a website. With few exceptions, no website needs to know your age, gender, profession, residential address or even your real name.

Tools I use

So how do we stop this? We make it difficult for them to listen to us all. This forces them have to try listen closely to each of us individually which means that mass surveillance is no longer a viable possibility.

There are some practical limitations between security and usability. The more technically complex the security measure, the harder it is for most people to use.

I installed Peerblock (www.peerblock.com) which keeps an up-to-date list of known bad guys online and prevents them from communicating with your computer. This blocks on a very low level and is a great starting point for securing your computer against unwanted visitors.

I made a number of changes to my browser as well. I disabled accepting cookies from third parties (people other than the specific website I'm visiting), as well as setting the cookie accept policy to ask me about every website I visit. Unless you need to log into a website, there should be no reason to accept a cookie from it. This prevents a large number of advertisers from being able to track and profile my behaviour across multiple websites.

I also installed a number of extensions for my Firefox browser:

- HTTPS Everywhere ensures that, where possible, I'm always on the secure version of a website (you're on the secure version when your URL starts with https://). This ensures that any information that passes between me and the website I'm on is encrypted. Download it at https://www.eff.org/https-everywhere.
- Adblock Plus (https://adblockplus.org) blocks intrusive ads and prevents my online behaviour from being tracked and profiled by large advertising companies.
- NoScripts prevents JavaScript from loading on each website I visit unless I explicitly indicate that I wish it to load. To show why I believe this is important, a visit to cnn.com loads advertising scripts from 5 other servers. This seems harmless enough, but since most of the top 10,000 websites have similar tracking, you'll often

How does Facebook make money? They don't charge you a fee to chat with your friends. The only metric they seem to care about is how many users they have. For them, users means money, because users are a product they sell. Those adverts in each page of Facebook are specially tailored to you based on what you write about, what type of photos you upload, where you live, what your interests are, what your religion, gender, level of education and who your friends are.

find the same scripts being loaded on radically different websites which allows advertisers to profile your behaviour based on the websites you visit.

- I also switched my browser's default search engine to https://duckduckgo.com/ which is a search engine that does not track or record your searches.
- I use customized version of SuperGenPass (http://www.supergenpass.com/) to generate a unique password for each site I visit, but there are less complicated tools available, such as LastPass (https://lastpass.com/).
- I use Truecrypt to encrypt sensitive files in Windows (http://www.filehippo.com/download_truecrypt/) such as tax returns, insurance claims, bank statements, contracts and private keys. This ensures that, if my computer is ever compromised, my personal details can not be used to facilitate identity theft. In Linux I use full disk encryption which ensures that, unless my computer is switched on and I'm logged in, all my files are securely encrypted. This is easy to setup when you install Ubuntu and only requires that you to check a box and provide a password which you will use to decrypt your files each time you boot up your computer.
- Tor (https://www.torproject.org/) is a tool to make you anonymous online by routing your internet activity through random computers dotted around the world. This tool is used heavily in countries where posting content online, that the government disagrees with, can lead to imprisonment. Tor, however, stops being useful when you use it to log into your personal Facebook account or you post any personally identifiable data. So use Tor when you want to be anonymous, not when you're doing your online banking.

I ditched plain SMS where I could. All SMSes are sent and stored in plain text which means the government has access to them. They also know exactly who you are as you're required by law to RICA your number. I replaced SMS with TextSecure on my Andriod which allows me to securely send messages to other friends with TextSecure installed, and normal SMSes to those without.

I also deleted my Facebook account. For many, this might seem like a drastic action, but consider this: How does Facebook make money? They don't charge you a fee to chat with your friends. The only metric they seem to care about is how many users they have. For them, users means money, because users are a product they sell. Those adverts in each page of Facebook are specially tailored to you based on what you write about, what type of photos you upload, where you live, what your interests are, what your religion, gender, level of education and who your friends are.

Now, you might ask yourself why you should make these changes. Surely if you have nothing to hide, I have nothing to fear? I ask you: do you have curtains? Using encryption and anonymising tools is like having curtains over your windows. At the moment, only a few windows have curtains on them, which makes governments very curious about what is happening behind them. The more people who add curtains, the more common is becomes, the less worth while it is for governments to try lift each curtain. It provides us with a herd immunity. The more of us who use them, the harder it is for all of us to be spied on. As an example of how a small change can have a large effect, Google changed Gmail and Google Search to only work over a secure HTTPS connection which effectively secured the email of 425 million users and ensured that no one can spy on over 5,922 million searches every day.

For a list of behaviour and software you can adopt to make it harder to be snooped on, visit https://pack.resetthenet.org/