DON’T BE AN INTERNET TURKEY

Snoopers
(or how to protect your data)

When Tim Berners-Lee was designing the technology that has transformed our world, he looked for a noun that would describe what he had in mind. The one he eventually settled on was "web", which is how the world wide web got its name.

To its inventor, the noun must have seemed perfectly apposite: it described the intricate, organic linking of sites and pages that he had in mind. But "web" has other, metaphorical, connotations. Webs are things that spiders weave with the aim of capturing prey. And if you want a metaphor for thinking about where we are now with networked technology, here's one to ponder.

Imagine a gigantic, global web in which are trapped upwards of two billion flies. Most of those unfortunate creatures don't know – yet – that they are trapped. After all, they wandered cheerfully, willingly, into the web. Some of them even imagine that they could escape if they wanted to.

We are those insects. The only way of escaping our predicament is to renounce the world in the way that Trappist monks once did. Since we're not going to do that, we have to face the reality: we're trapped in a system in which everything we do is monitored and logged and in which privacy is a thing of the past. Everything that you do with modern communications equipment leaves a digital trail. And this trail is followed assiduously not just by giant corporations, but also by governments and their security services – as vividly illustrated by the revelations of Edward Snowden.

What's astonishing is how unconcerned many people appear to be about this. Is it because they are unaware of the extent and comprehensiveness of the surveillance? Or is it some weird manifestation of Stockholm syndrome – that strange condition in which prisoners exhibit positive feelings towards their captors? What we've learned above all from the Snowden leaks is that the scale and capability of the NSA surveillance are much greater than anyone imagined. Most people had assumed that most non-encrypted communications were vulnerable and some speculated that some encrypted communications (eg Skype) had a hidden backdoor for the NSA. But nobody realised that, as the latest revelations showed, all the encryption technologies routinely used to protect online transactions (https, SSL, VPN and 4G encryption), plus anything going through Google, Microsoft, Facebook and Yahoo, have been cracked.

What this means is that no form of electronic communication handled by commercial companies can now be assumed to be secure. In that sense, the NSA has really fouled the nest of the US internet industry . And it is even suspected that about 90% of communications routed through the TOR network are using encryption that may also have been hacked by the NSA. What can you do if you're someone who feels uneasy about being caught in this web? The honest answer is that there's no comprehensive solution: if you are going to use telephones (mobile or landline) and the internet then you are going to leave a trail. But there are things you can do to make your communications less insecure and your trail harder to follow. Here are 10 ideas you might consider.

1 Email

Rethink your email setup. Assume that all "free" email and webmail services (Gmail etc) are suspect. Be prepared to pay for a service, such as Fastmail,that is not based in the US – though some of its servers are in New York with backups in Norway. (My hunch is that more non-US email services will appear as entrepreneurs spot the business opportunity created by the Snowden revelations.) It would also be worth checking that your organisation has not quietly outsourced its email and IT systems to Google or Microsoft – as many UK organisations (including newspapers and universities) have.

The real difficulty with email is that while there are ways of keeping the content of messages private (see encryption), the "metadata" that goes with the message (the "envelope", as it were) can be very revealing, and there's no way of encrypting that because its needed by the internet routing system and is available to most security services without a warrant.

2 Encryption

Encryption used to be the sole province of geeks and mathematicians, but a lot has changed in recent years. In particular, various publicly available tools have taken the rocket science out of encrypting (and decrypting) email and files. GPG for Mail, for example, is an open source plug-in for the Apple Mail program that makes it easy to encrypt, decrypt, sign and verify emails using the OpenPGP standard. And for protecting files, newer versions of Apple's OS X operating system come with FileVault, a program that encrypts the hard drive of a computer. Those running Microsoft Windows have a similar program. This software will scramble your data, but won't protect you from government authorities demanding your encryption key under the Regulation of Investigatory Powers Act (2000), which is why some aficionados recommend TrueCrypt, a program with some very interesting facilities, which might have been useful to David Miranda.

3 Web browsing

Since browsing is probably what internet users do most, it's worth taking browser security and privacy seriously. If you're unhappy that your clickstream (the log of the sites you visit) is in effect public property as far as the security services are concerned, you might consider using freely available tools such as Tor Browser to obscure your clickstream. And to protect yourself against the amazingly brazen efforts by commercial companies to track your online behaviour you should, at the very minimum, configure your browser so that it repels many of these would-be boarders.

4 Cloud services

The message of the Snowden revelations is that you should avoid all cloud services (Dropbox, iCloud, Evernote, etc) that are based in the US, the UK, France and other jurisdictions known to be tolerant of NSA-style snooping. Your working assumption should be that anything stored on such systems is potentially accessible by others. And if you must entrust data to them, make sure it's encrypted.

5 File storage and archiving

An option that an increasing numbers of people are exploring is running their own personal cloud service using products such as PogoPlug and Transporter that provide Dropbox-type facilities, but on internet connected drives that you own and control. And if you carry around confidential data on a USB stick, make sure it's encrypted using TrueCrypt.

6 Social networking

Delete your Facebook account. Why do the CIA's work for it? And if you must use it, don't put your date of birth on your profile. Why give identity thieves an even break? And remember that, no matter what your privacy settings, you don't have control over information about you that is posted by your "friends".

7 Location data

Avoid using services such as FourSquare that require location information.

8 Wireless services

Have Bluetooth off by default in all your mobile devices. Only switch it on when you explicitly need to use it. Otherwise you'll find that even a dustbin can snoop on it. Similarly, beware of using open wifi in public places. At the very minimum, make sure that any site you interact with uses HTTPS rather than unencrypted HTTP connections. If you don't then anyone nearby can use Firesheep to see everything you're doing.

9 Personal security

Forget password, think passphrase – ie a meaningless sentence that you will remember – and do some transformations on it (first and third letters of every word maybe) so that you can generate a stronger password from it every time. Or use a passwordmanagement app like LastPass or 1Password. And if a service offers multi-factor authentication, make use of it.

10 Search engines

All the big search engines track your search history and build profiles on you to serve you personalised results based on your search history. if you want to escape from this "filter bubble" you need to switch to a search engine that does not track your inquiries. The most obvious one is the bizarrely named but quite effective DuckDuckGo.

http://www.theguardian.com/technology/2013/sep/16/10-ways-keep-personal-data-safe