Online security in a post Snowden and “Snoopers Charter” world

Edward Snowden opened to door into the mass surveillance of digital communications by the security forces around the world. Initially this was met with disbelief by the public, but led to public disclosures of some of the tactics by some of the agencies involved – enough to indicate the validity of the overall claims. The charm offensive by governments has provided a groundswell of public belief that snooping on everyone’s digital communications is a good thing that stops terror and crime. The “Snoopers Charter” is the UK embodiment of this belief.

So what is the law (current and planned)?

As the Snowden revelations revealed, GCHQ was already collecting and storing far more of our data than we realised. The new legislation, introduced to parliament on 4th November 2015, is an attempt to bring this surveillance under a legal framework. This is the “Snoopers Charter” MkII (the Investigatory Powers Bill) – MkI (the Digital Communications Bill) having been blocked by the minor government coalition partner in 2013.

The current legislation in this area is the Regulation of Investigatory Powers Act (RIPA), which was passed in 2000. The rise of digital means it's already hideously out of date. David Anderson QC, the independent reviewer of terrorism legislation, has said that the current system of laws is "undemocratic, unnecessary and in the long run intolerable".

In 2014, after the failure of “Snoopers Charter” MkI, parliament rushed through the Data Regulation and Investigatory Powers Act (DRIPA), an emergency piece of surveillance legislation, but it didn't last long - a year later, its first two sections were ruled illegal by the High Court as it was "inconsistent with European law". The government was given until March 2016 to come up with replacement legislation, hence the slightly confusing state of play now.

Theresa May has confirmed that under the newly proposed bill the security services won't be able to look through your complete browsing history - instead, they'll have access to the domains (web sites, not individual pages) you visited and when. Similarly, it's predicted that they'll be able to see who you texted and emailed, but not the content of those messages. It is likely, though, that the law will force companies to store our data for a minimum of 12 months (and at our costs).

But the Daily Telegraph say, “[we] understand that a total of 38 bodies will also be entitled to access the records for the purpose of "detecting or preventing crime".” Using the existing RIPA, Town halls were granted permission to access private communications data 2,110 times last year (2014), more than GCHQ and MI6 combined. David Davis MP said: "It is a serious amount of information. I don't think that the British public want councils to have access to this."

In the wake of the horrendous attacks in Paris, there will be even more backing for the view put forward by the security forces in the run up to the introduction of the bill. Namely, that the security forces need to intercept all of your electronic communications to prevent these atrocities on British soil.

If you don't want this level of official snooping you need to write to our MP Chris Heaton-Harris at http://www.heatonharris.com

Why do we need to protect ourselves from this snooping?

Have you ever researched sexual health, mental health or similar topics before discussing the topics with friends or family? Then would you like your life insurance company to know you have viewed an Aids or depression site when they are planning your next renewal? Insurance companies already have 'anonymised' health information from the NHS databases, unless you opted out. (It has been proven that relatively simple cross referencing with other data sources can identify the health records with individuals.)

How many times have you clicked on an innocent looking link, only to find that the website it jumps to is anything other than innocent? Do you want classifying based on an accident?

On a wider scale, have you ever read the T&C's of Google, Facebook, etc. To paraphrase slightly they say "we will gather any data we want, from anything you put on our service, to provide you with a more targeted experience". Their aim is to know more about you than you do. Have you looked at something on Amazon one day, and found it keeps popping up in adverts on unrelated web sites over the next few days?

Windows 10 sends information almost constantly back to Microsoft, and there are reports that this behaviour is also appearing on Windows 7 and 8 as "critical security updates"!

Are you happy with this gathering of information about you, your searches, your purchases, your jokes with your friends, by all and sundry?

So what can we do to protect ourselves?

The basics

Any defence is only as good as its weakest point and hence any good defence has many layers to it.

The first layer is to stop much of the Internet from actually entering your network via a firewall, such as is built into most broadband routers (including the one from Gigaclear). Windows has its own firewall that has been turned on by default since Windows XP release 2.

The next layer is to have a good antivirus – this does not mean that it necessarily has to be expensive, as most of the popular products have a commercial version and a similarly capable free version. (Beware as some including AVG have now started harvesting and selling browsing data.) Windows 8 and 10 have an antivirus built in called Windows Defender which although not leading edge is quite reasonable. If you think that you may have a virus, or as a regular precaution, you can run a tool such as Malwarebytes Anti-Malware's scanner which detects and removes malware like worms, Trojans, rootkits, rogues, spyware, and more.

The next layer is protection for your browser itself. Popular software programs contain millions of lines of code. Bad guys exploit flaws (vulnerabilities) in the code to deliver malware. Malwarebytes Anti-Exploit or similar tools wrap extra layers of security around popular browsers, preventing exploits from compromising vulnerable code.

The next layer is something to help in avoiding access to known ‘bad’ web pages. There are two forms of this (a) a program that actively runs on your computer called a “Net Nanny” or (b) a facility at the DNS server (the part of the Internet that converts the name you use for a website into the number notation the network uses) that does not perform the required conversion for sites it has listed as bad. The Gigaclear network uses “Open DNS” to provide the blocking.

The next layer involves you and the tricks that criminals will try and play on you. Some of the things to watch out for are:

- Take care with email attachments – if it is from someone you don’t know, or unexpectedly from someone you do know, do not open it.
- Take care with links in emails – only follow them if you are really confident in the person or company who sent them to you.
- With either of the above, the company or friend will never mind you ringing to check before taking action.
- If something sounds too good to be true, it invariably is. There are no African funds to transfer etc.
- Your bank or random people will not ring to help you sort out your PC, just put the phone down on them.
- Your bank will never ask for account details from you, either online or on the phone.

- Give out no information to cold callers. They are extremely skilled at getting seemingly innocent information from you. You do not have to speak to them or answer their surveys.
- If a website is asking for personal detail check that it is marked as secure by your browser (this is often a green padlock next to the website name starting with "http**s**".)
- Be careful how much you disclose online.
    - How good is your bank security question of "what's the colour of your first car" if you have a picture of it plastered all over your Facebook account?
    - Have you noticed that Facebook wants to tag your friends based on its image recognition of the photograph you just uploaded, and at least one of them will have listed their first school on there. It's also quite likely that the school is in the town where you were born.
    - If your name is Smith and many people in your friends list are named Wilson, there is a good chance that these are cousins and Wilson is your mother's maiden name, so don't use that as your bank security question.
    - If you have your mobile phone GPS turned on and you take many photographs over time from the same location, there is a good chance that it is your home.
    - This type of social engineering only takes minutes, and very little more is required to take control of your online life.

The next level

- Most people use Google as their search engine. Could I suggest using www.startpage.com which anonymises your searches through their secure proxy service – you get the same results from Google, but they see the requests coming from Startpage rather than from you. (But once you follow a link to a web site, that site will be able to see you – I don't know of a good, free proxy for that, yet.)
- Don't use Chrome, as although it is one of the best browsers, it is owned by Google. I am currently using Firefox.
- A great source of irritation to many people are the advertisements that appear on many pages, some of which could contain malicious code, or links to 'unsafe' websites. These can be blocked by the use of an ad blocker – my choice is uBlock at https://addons.mozilla.org/en-GB/firefox/addon/ublock-origin, as other blockers are paid by Amazon, etc. to allow their adds through!

  Also many of the websites that serve the ads are very slow, causing severe delays in page loading and spoiling the whole browsing experience.
- HTTPS Everywhere is a Firefox extension to protect your communications by enabling HTTPS encryption automatically on sites that are known to support it, even when you type addresses or follow links that omit the https: prefix. It is available at https://addons.mozilla.org/en-GB/firefox/addon/https-everywhere
- Be smart with your security questions. See earlier note about disclosing too much information online. The key is to mix things up as much as possible so if someone does get into one of your accounts, they can't use the same information to get in everywhere else.
- Use a password manager. It doesn't matter how many surveys and reports come out that tell people to use different passwords and complex passwords, a huge percentage of the population maintain borderline idiotic approaches. The simple answer is: get a password manager or vault. It will protect you. Use one long, but memorable, password to access the vault and store all your usernames and passwords in there. (And back it up on a regular basis!)
- Use two-factor authentication. Many services such as Gmail, Twitter, Dropbox, Hotmail, and Facebook offer this now for no charge. So even if your password does get exposed, you still have a backup such as a text message to your phone to secure your information.

Want to go further?

Edward Snowden was the whistle-blower to the exploits of the NSA, GCHQ and other security organisations. He recently gave an interview to "The Intercept" (an online magazine) at https://theintercept.com/2015/11/12/edward-snowden-explains-how-to-reclaim-your-privacy which forms the basis of the advanced security protections suggested below.

So, if you regularly feel the need to line your hat with tin foil, or trap a hair in your office door when leaving, you can try these more extreme measures.

- Use Tor when browsing. You don't have to use Tor all the time (it does slow things down considerably and some sites will also block Tor traffic). But if you are looking at, or for, something that you feel is sensitive, then either set up your browser to work with Tor or use the Tor browser. Despite what senior Police and government officials claim, using Tor (The Onion Router) is certainly not illegal. In normal use it just routes your Internet access through various proxy computers to hide your true identity; exactly the reason it was set up by the US government for its own use. Legitimate uses also include journalists and NGO's working in foreign countries, often in conjunction with SecureDrop or similar tools.

- Use a secure hypervisor and a different virtual machine for differing aspects of your life. (Or more simply, run your browser from a bootable USB stick such as https://tails.boum.org)

- Encrypt your hard drive. This is comparatively easy these days but you have to be careful to do two things: one, have a longish phrase to make it worthwhile; and two, make sure you remember that phrase. There will be a slowdown in performance but nothing too bad if you have a modern machine.

  Remember that under Regulation of Investigatory Powers Act 2000 (RIPA) you are obliged to give the encryption key upon demand to Police Officers under penalty of 2 years (or 5 in terrorism cases) in jail. It was proved in the Appeal Courts in 2008 that this key is an item in itself (even if it's just in your memory) and so self-incrimination protection does not apply.

  Also note that this is really only much use against someone who has physical access to your PC (or laptop left on the train, or hard-drive sold on Ebay, if you are a government or health service employee!). When you legitimately start to use the encrypted drive, the contents of that drive become visible to any malware that is already on your PC.