NEWSANALYSIS

The Linux Voice view on what's going on in the world of Free Software.

The surveillance state

We are being spied upon more than ever – but this truth has been twisted and denied by some.

Simon Phipps
is president of the Open Source Initiative and a board member of the Open Rights Group and of Open Source for America.

As revelations from the whistle-blowing by Edward Snowden continue to flow, activists increasingly say we are the subjects of extensive, even blanket surveillance. The UK government vigorously denies this, saying we do not live in a surveillance society. It turns out both are right -- here's why.

GCHQ, the NSA and probably every other intelligence agency worth the name are actively gathering data from the internet. Everything on the internet is transient, with different decay periods, so gathering information is a constant process. They believe everything that can be gathered without illegal action is fair game, so they gather anything and everything they can, storing it just in case.

They are without doubt capturing and recording all and any email, instant messages, web pages, social media traffic and so on. Recent disclosures (**www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data**) reveal that the NSA collects "nearly everything a user does on the internet" and then offers analysts tools to search the data thus cached.

They have a variety of explanations why it's all legally gathered. Some is on open websites. Some is "public" in the sense that it passes through unsecured intermediaries that anyone could theoretically observe. Some is private, but can be gathered because of their interpretation of certain legal doctrines ("sent abroad" for example, when the service provider is in a different country to the originator), which allows them to treat it as public.

Public or private?

Intelligence agencies are thus slurping up enormous quantities of data in a wide range of protocols and contexts, far more than could ever be appropriate for any investigation. Why are they doing this? Because otherwise the data would be lost by the time they knew they needed it. They are not actually looking at most of it, at least not straight away. All they are doing is making transient data persist – they are caching. They are not breaking any rules by doing so (at least according to their own legal outlooks). They are simply engaged in blanket data gathering to the limits of the legality they understand for their acts. The result is truly enormous "data lakes".

To *study* the data is a different thing, in their view. According to their legal advisors "wire tapping" or "hacking" starts at the point they actually have a human being analyse or interpret the data. The NSA's XKeyscore tool provides such a capability, and undoubtedly GCHQ and other agencies have similar tools for fishing in their own data lakes. They claim that access to the lake is limited, but

disclosures suggest that it is limited by rule and the threat of audit, and not actually by any technical means. As a consequence, agents have to consciously ignore out-of-scope results from tools like XKeyscore.

Let's go fishing

Using metadata is considered OK as it is simply the 'public' aspect of the contents of the data lake. Metadata helps target the fishing more accurately, but it can also be used to 'triangulate' and determine facts directly. It's an open question whether using varied metadata to triangulate on private facts is surveillance.

So when Theresa May says "there is no programme of mass surveillance and there is no surveillance state" and responds to claims that GCHQ engages in unlawful hacking as "nonsense", she is probably speaking the truth according to her chosen frame of definition (in the same sense as Bill Clinton's statement "I did not have sexual relations with that woman" was true). There is certainly a well-considered system of rules that make her statements precisely true.

Her denial is still disingenuous. Most people would expect her words to mean no surveillance is happening. But a vast lake of data is being "persisted" for future analysis, and a large quantity of metadata is also retained to decide where in the lake to go fishing. Her attempt to divert us from this truth is itself a signal of a problem.

The intelligence services and the public officials they hide behind know we would be alarmed both by the volume of data they hold on us and by the way it is manipulated and would rather we stopped asking questions. That's exactly why we need organisations like the Open Rights Group and the Electronic Frontier Foundation to keep asking.

> **"Everything on the internet is transient, so gathering information is a constant process."**

Raspberry Pi • Russians • OwnCload • Ardour • Allseen Eye • Linux Extremism

CATCHUP

Summarised: the biggest news stories from the last month

1 Raspberry Pi Model B+ adds USB ports, micro SD
Mere nanoseconds before we went to press, the Raspberry Pi Foundation announced an updated board: Model B+. This adds more GPIO pins (taking the total to 40), two extra USB ports, and a micro SD card slot. The board is now neater and smaller, and much work has been done to make it less power hungry: "we've taken between 0.5 and 1 watt of power consumption out of the device", Liz Upton told us. Stay tuned for more on the Model B+ next issue!

2 Russian government to ditch Wintel for Linux
It's all getting a bit Cold War-esque, with increased tensions between the West and Russia over Ukraine. Now the Russian government has announced a change in policy from 2015 onwards: its departments will no longer buy PCs with Intel or AMD chips running Windows, but systems based on the home-grown Baikal CPU. Moreover, Linux will be the standard operating system. The Kremlin expects to buy 700,000 PCs with the new setup next year – a big migration to Linux.

3 OwnCloud 7 Beta sports new features galore
We're big OwnCloud fans here at Linux Voice HQ, and this snapshot of the upcoming version 7 has plenty to explore. The interface has been refined, there are new sharing features, and the Documents editor gets annotations and Microsoft Word support. Full details at: **http://tinyurl.com/oe3wr7n**

4 Ardour digital audio workstation low on cash
Many Free Software and open source projects survive solely from donations, and that's how Ardour has kept going over the years. The lead developer has said he doesn't like begging for more money, but as donations have slowed down in recent months, he's finding it hard to keep working on the application full time. If you're an Ardour user, you can help out by taking out a subscription that helps to fund features and documentation: **http://tinyurl.com/meg4cyd**

**5 Microsoft joins AllSeen Alliance, a project from The Linux Foundation**
Is this post-Ballmer Microsoft going to be a better player in the FOSS world? It's too soon to tell, but the previously GPL-dissing company has just joined the AllSeen Alliance, a group effort to create an open source platform for the "Internet of Things". The Alliance was kickstarted by The Linux Foundation, and now counts LG, Sharp, Panasonic, Cisco, D-Link, HTC and other big-name companies as members. **www.allseenalliance.org**

6 100+ GitHub repositories taken down after DMCA notice from Qualcomm
Lawyers at wireless networking giant Qualcomm have thrown a hissy fit over alleged copyright infringement on GitHub. Over 100 projects on the popular code-sharing site have been taken down, including a CyanogenMod repository, but the justification has been controversial, as many GitHub developers claim that they're only using code and specification documents originally made free by Qualcomm itself. **http://tinyurl.com/pptf686**

7 Automotive Grade Linux issues first release
In other Linux Foundation news, the first version of Automotive Grade Linux is available to download. This is a "Linux-based software stack for the connected car", designed as a reference implementation for car makers to build upon. It features Google Maps integration, media playback, Bluetooth phone connectivity and a snazzy user interface. The stack has solid backing: Intel, Fujitsu, NEC, TI and Toyota, among other companies. **http://tinyurl.com/o24h7az**
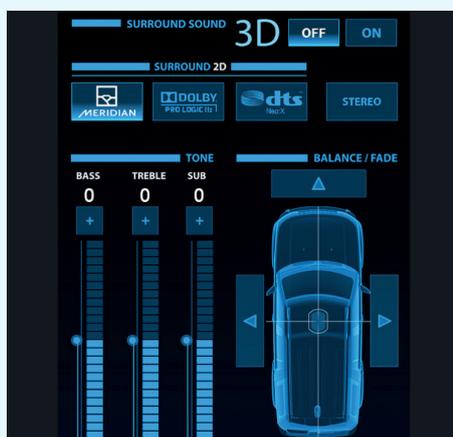
8 Use Linux? You might be an "extremist", says NSA
If you've ever been to the Tor website, tried the Tails distro or even done general web searches for software that provides privacy or anonymity, the NSA may be tracking you. Yes, new leaks have shown that the US spying operation regards Tor and Tails as tools advocated by "extremists", and even places where they're discussed, such as Linux forums, are labelled in the same way. So just visiting Linux-related sites can have the spooks following you. Time for a new internet, we thinks…