NEWSANALYSIS

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

Opinion

"...and the filters don't work/ they just make it worse..."* *sincere apologies to The Verve

Web filters to protect children from dodgy online content don't work. Here's why.

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

The UK government has pressured ISPs into applying content filters to their customers' connections, in the name of protecting children from unsuitable content. During 2014, ISPs will be approaching their customers and trying to persuade them to turn on filtering. But this is a mistaken approach arising from magical thinking – "this thing should exist so it must be possible". Content filters can't work, for several reasons:

For the most part they can be avoided. Techniques such as using a freely-available VPN tool such as TunnelBear, or switching to non-ISP DNS enable users to effortlessly route round filters. As a consequence, relying on filters to do your parenting for you is foolish. Not only are they no substitute for parental oversight and care, they inculcate a careless reliance.

They attempt to make objective a task which is subjective. For example, some people will regard websites promoting gay rights or giving information about abortion as unsuitable, while others will treat both topics as essential resources. Who gets to decide for us all? The answer in most cases is "nobody knows", since the ISPs are largely buying the blocking facility from third party suppliers rather than building it themselves. Statements by filtering advocates take it as read that there's a consensus on what's bad are deceptive.

I'm sorry Dave, I can't do that

The government proposes a whitelist of sites that should never be blocked, but this approach is flawed too; partly because their vision of which sites should be whitelisted only includes obvious, politically appealing cases like child welfare charities, omitting to mention harder cases such as mutual-support groups, political comment and satire and completely ignoring the sort of free speech cases that are politically unappealing to the government. Indeed, a comprehensive whitelist is probably impossible, because the internet, like space, is vastly, hugely, mindbogglingly big.

Even if a whitelist could work, most content providers won't know they should be on it as blocking is invisible to them. Since the filter service is applied by ISPs to their customers' connections as part of the service, they rely on customers raising the alert on overblocking. As a web page provider, I have no way to know whether a given ISP is blocking my site, and when I eventually find out there's no deterministic way to get it fixed since neither the ISP nor their third-party provider have any duty to help me; in fact, the ISP's contract with their supplier may actually prohibit them from helping me.

Most content providers might not even think to check anyway, even if there were a way to do so. Recently, the jQuery website was added to the block list for UK ISP Sky after the domain was mistakenly listed in the "malware and phishing" category. This unexpectedly broke many websites, since over three-quarters of the top 10,000 websites use **jquery.com**-hosted components. A church website in Sheffield was blocked; my own company website was blocked. The robots that do the ranking can take potshots at pretty much anything, and only the customers of the ISP involved could ever know.

Think of the children!

Meanwhile, parents are lulled into a false sense of security. The web is something of a mystery to many, and the assurance that "parental control filters" are keeping their children safe may well reduce the urgency of understanding how to supervise children on the web. The correct path is sitting with children, assisting their use of technology, explaining how to decide who to trust, explaining when to ask for help or permission, applying discipline wisely.

If it were possible to magically determine the suitability of any random website for any random web user, and if filtering could be made uncircumventable without destroying the utility of the internet, maybe it would be OK to have a censorship switch that parents could flip. But none of that is possible, and the facilities we're being sold will do more harm than good. You can help; check out **blocked.org.uk**. That will help practically, and also fuel the political battle.

"The government proposes a whitelist of sites that should never be blocked, but this approach is flawed."

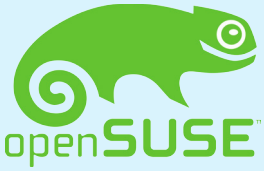
SUSE • Firefox 27 • Valve • Tizen • Developers • OpenSSH • Chakra Linux • Kernel

CATCHUP Summarised: the nine biggest news stories from the last month

1

SUSE announces live kernel-patching system

Imagine being able to patch your kernel without having to reboot. And imagine the staggering uptimes you'd be able to achieve... A few methods have been developed to do this, but they have never made it into the mainstream kernel. Now the SUSE team has announced kGraft, with a first release due in March. **http://tinyurl.com/susekgraft**.



2

Firefox 27 released

Given the break-neck pace of development in Firefox, it's hard to keep track of all the new features. Firefox 27 enables you to run more than one service at a time with its Social API (so you can get notifications from multiple sites), and also enables support for TLS 1.1 and 1.2 by default. SPDY 3.1 is included too.

3

Valve offers free games to Debian developers

SteamOS, Valve's gaming platform based on Debian, could massively shake up the computer games market. Users will be able to play Valve's ever-growing range of titles without having to even boot Windows. A healthy relationship between Debian and SteamOS is important, so Valve is now offering free subscriptions to Debian developers.

4

First Tizen smartphone leaked

We've seen a bunch of Linux-based mobile platforms come and go – Maemo, Moblin and Meego – and now we have Tizen. The Samsung ZEQ 9000 will be the first phone to run this operating system, sporting a 4.8-inch display and a 2.3GHz processor. Physically, the phone looks a lot like the current Galaxy range; it's due for launch later in the year.

5

80% of kernel developers are paid

Every year the Linux Foundation tracks changes to the Linux kernel source tree, and determines how much code is being contributed by commercial companies. Newly released stats show that over 80% of developers are being paid to work on the kernel, with Red Hat, Intel and Texas Instruments the three biggest contributors.

6

OpenSSH 6.5 released

You'd think OpenSSH is secure enough already, what with it being a product from the OpenBSD camp, but given the NSA spying revelations you can't be paranoid enough. Version 6.5 includes new cyphers and key types, to reduce even further the chance of someone peeking at your remote login sessions.

7

Chakra 2014.02 available

With most distros you upgrade once or twice a year and get a bundle of new stuff. There are also rolling-release distros such as Arch, which give you a constant stream of new software. Chakra uses a "half-rolling release" model: the base system is updated only after extensive testing, whereas new desktop apps flow in all the time. **www.chakra-project.org**

8

Kernel 3.13 brings new packet filter

One of the biggest new features in kernel 3.13 is nftables, the successor to iptables. This is a "packet classification framework" – ie, a system for choosing where network packets go, as used in routers and firewalls. Nftables compiles rules down to pseudo-bytecode, and promises to make life easier for administrators thanks to a simpler syntax.

9

2014: the year of code

After more or less being shamed into action by the efforts of Code Club, Young Rewired State and the Raspberry Pi, the UK government has launched something called the Year of Code, which is supposed to encourage more people to learn to program. According to the website, 1 in 6 adults lack digital skills, though what this actually means is anyone's guess.