British government introduces Internet censorship filters

Mark Blackwood
7 August 2013

Complying with the dictates of the Conservative-Liberal-Democrat coalition government, the UK's biggest Internet Service Providers (ISPs), covering 95 percent of all households, have agreed to initiate a "family-friendly" filtering system for the Internet. Smaller ISPs are expected to follow suit. The government will consider legislation if the self-regulatory agreement does not work.

Using the supposed threat of paedophiles as a pretext to attack basic democratic rights and bring in broader censorship, Prime Minister David Cameron declared last month, "The actions we're taking today come back to that basic idea: protecting the most vulnerable in our society, protecting innocence, protecting childhood itself. That is what is at stake, and I will do whatever it takes to keep our children safe."

By the end of 2013, anyone setting up a new broadband account will have the filters automatically switched on by default, which will block all online material the British government deems objectionable. Users who wish to view "objectionable" material will have to opt in. The system will be extended to all existing users by the end of 2014.

According to the civil liberties organisation Open Rights Group, the filters will not just block pornography but "also restrict access to sites deemed unsuitable for under 18s including information on alcohol and other drugs, forums, YouTube and controversial political views."

The group points out that adult filtering will also be applied along the same lines. Any web site containing too many blacklisted words including terrorism, weapons, violence, depression, war, and Taliban could also find access from British Internet users prohibited. Should this be the case, the *World Socialist Web Site* could in all possibility find itself included on the censorship hit list.

Wikipedia co-founder Jimmy Wales, who is also one of Cameron's technology advisers, has declared the filter "an absolutely ridiculous idea" and insisted that the software necessary to implement the policy would not work.

He went on: "Additionally when we use cases of a paedophile who's been addicted to child porn videos online, you realise all that Cameron's rules would require him to do is opt in and say, 'Yes, I would like porn please'."

Wales is missing the point. Under the new system the government will determine what is or is not objectionable on a whole range of subjects, not just pornography. It will possess the capacity to collect detailed information of an individual's filter options and generate a comprehensive database for profiling all UK web users.

Numerous Internet forums, including the BBC's web site, have been flooded with statements displaying the response of many within the British public.

"It's not about porn. Never was. What next, foreign news sites? Political forums? Social media? The day they start to censor the Internet will be the day that the revolution starts," writes one individual.

"Porn today, articles criticising the current regime next. How would we know?" remarks another.

The UK government's attempt at broadening Internet censorship does not end with the "opt-in" button on a customer's broadband account. Web site owners and bloggers who attempt to avoid the government's filter will be confronted with one of two options—self-censorship or being blocked. Anyone trying to get around the filter will likely be identified, recorded and subjected to extensive network surveillance and online traffic analysis, and face the possibility of an array of allegations.

The government's firewall is set to block access by default to web censorship circumventing tools, such as proxy servers and virtual private networks (VPNs). It is highly likely that restricted access to the Tor software bundle, which is free software enabling greater anonymity

and connects to the heavily encrypted Tor Network, will also be contained within the censorship filter.

Unsurprisingly, the Tor network is used extensively and enjoys a trusted reputation internationally as a means to defend protesters and political dissidents against the network surveillance and traffic analysis employed by totalitarian regimes. Since the revelations by US whistle-blower Edward Snowden of the mass state surveillance programs carried out by the US and UK governments, the use of VPNs and Tor has skyrocketed.

Due to the elevated levels of encryption employed by VPNs in general and Tor in particular, the monitoring of a person's Internet activities by the state becomes more difficult. These technologies can inhibit an ISP from collecting data on a person's online activities and connect it to his or her name, address, age, phone number, etc., which is why they have become so popular.

Some indication of the implications of the new filter was revealed in an investigation carried out by the Open Rights Group (ORG) of mobile phone companies in the UK, which already operate a similar system to block Internet access. In January-March 2012, ORG reported that not only had its own site been blocked, but 60 other sites had told them they had also been blocked at some time in those three months, including a number of those that lean towards the left end of the political spectrum. A full list in Excel format can be downloaded.

Together with the information made available by Edward Snowden, Cameron's latest move is a clear indication of the British state's advanced preparations to implement dictatorial rule. The working class must recognise the grave dangers that lie ahead. Rather than relying on VPNs and proxies, what is required above all else is the building of a mass revolutionary party armed with a socialist political perspective.