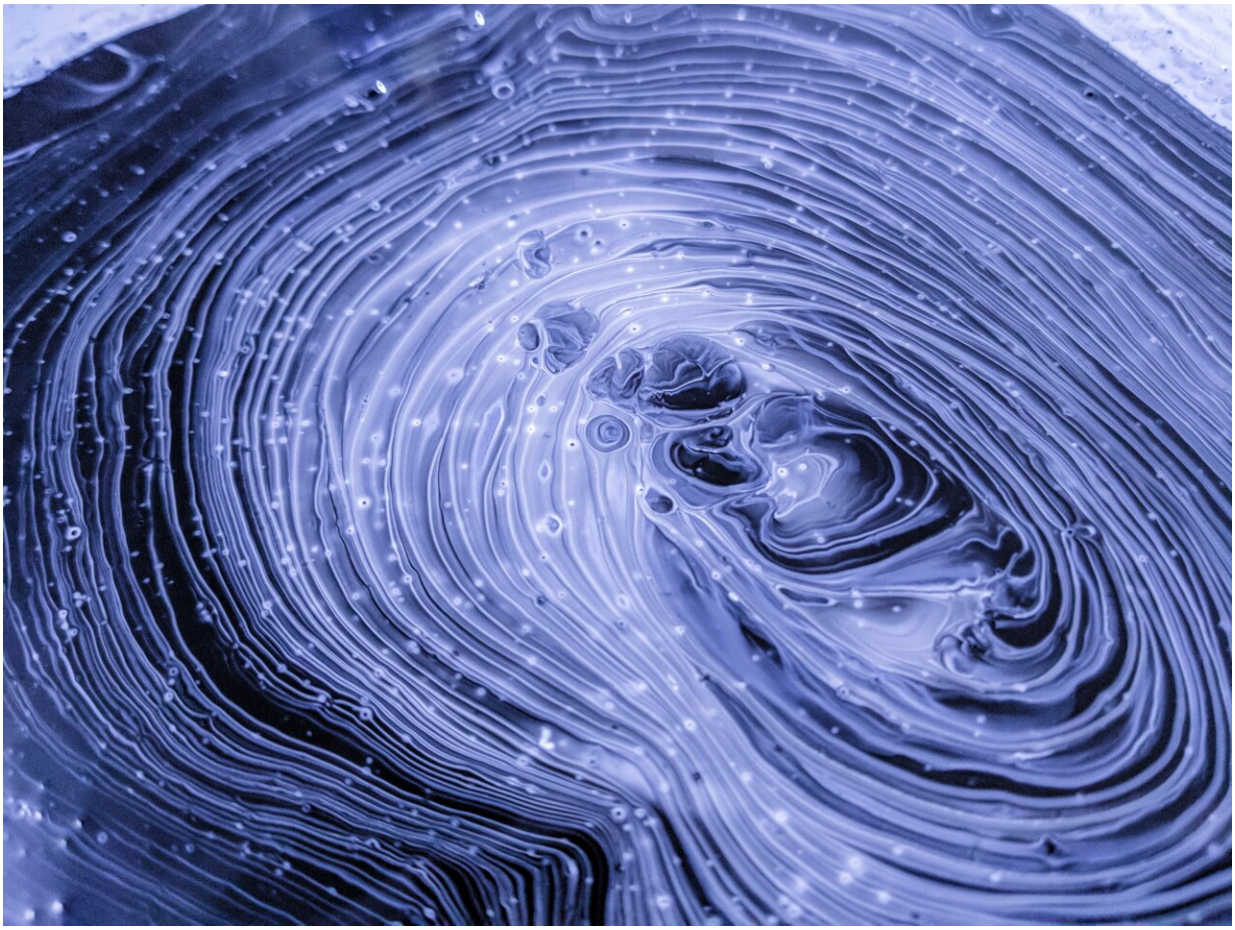
Why you should care about China's VPN crackdown

August 23 2017, by Omair Uthmani



Credit: CC0 Public Domain

Internet censors have a new target. The Chinese and Russian

governments recently announced plans to block the use of "virtual private networks" (VPNs), which are a key tool for people trying to avoid internet restrictions and surveillance.

This crackdown isn't surprising, given the two countries' histories of monitoring their citizens and blocking certain websites and online services. But it raises the question of whether other governments will follow this lead and introduce their own VPN bans, especially given how VPNs currently allow citizens to avoid the extensive internet surveillance that Western governments practice.

China and other countries block many websites they don't want their citizens to access, including sites such as Twitter and YouTube that allow users to freely post almost anything they like. But Chinese internet users wishing to evade these restrictions can currently use VPNs to visit these sites, because they provide access via a separate encrypted server that can't be monitored by the government.

Since Chinese internet service providers only filter out connections to the likes of Twitter and YouTube, users can still connect to sites which offer VPN services. VPN acts like a proxy, accessing the banned sites on the users' behalf and allowing them to effectively bypass the restrictions, as well as avoiding government snooping. But now the Chinese government has ordered national telecommunications firms to block VPNs as well from February 2018.

Russia doesn't block access to as many sites as China. It allows access to Facebook and Twitter, for example. But it still practices significant internet censorship. And now it has followed China's lead by also restricting VPN services, stating the measure is intended to clamp down on anonymous access to unlawful content.

These events come as little surprise given China and Russia's track

records. China, in particular, has introduced a number of similar restrictions on VPNs in the past. These clampdowns were vigorously enforced for a period of time and then relaxed.

Although the new restrictions seem to be more comprehensive, it's worth noting that they may also be temporary, with the official statement indicating that the measures would run until March 31, 2018. This may have something to do with the 19th National Congress of the Communist Party of China being held in Beijing in the autumn of 2017.

It's also worth pointing out that both China and Russia are heavily invested in developing their industries and economies and keenly aware that this cannot occur without businesses and researchers being able to access internet resources. Xi Jinping, the Chinese president, stated at the Davos economic summit in January 2017 that he wanted to "redouble efforts to develop global connectivity". This must include access to the internet.

However, there is significant concern from internet anti-censorship organisations that these kinds of events indicate a growing global trend. Governments are increasingly monitoring, restricting or censoring the internet activities of their own and other nations' citizens.

This trend includes most major Western governments. For example, the US National Security Agency (NSA) and the UK's Government Communications Headquarters (GCHQ), have been the subject of considerable debate for their practices of internet snooping and the mass collection of citizens' data.

Western laws are vulnerable to VPNs

If the recent laws in China and Russia are alarming, so too are those such as the US Executive Order 12333, authorising the collection of data

inside and outside US borders for "national security purposes". This order permits the collection and storage of communication metadata and content without a warrant, court approval or reporting to Congress.

The UK's Investigatory Powers Act 2016 isn't far behind, requiring internet service providers to keep a full list of users' connection records, including a list of every website that people have visited, for a year. The UK government has also announced plans to restrict access to pornography to over-18s and ban material it deems harmful altogether, something China has done for years. A major flaw in all these plans is that the surveillance and restrictions can be bypassed using a VPN.

While the restrictions on VPN services in China and Russia may be temporary in nature, they do form part of the increasing appetite of governments the world over to monitor and limit the activities of internet users. If Western governments begin to see VPNs as a threat to their own internet regulation, there's a real chance they could follow the lead of China and Russia and introduce their own bans. Online privacy could be a concept heading for extinction.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: Why you should care about China's VPN crackdown (2017, August 23) retrieved 18 April 2024 from https://phys.org/news/2017-08-china-vpn-crackdown.html