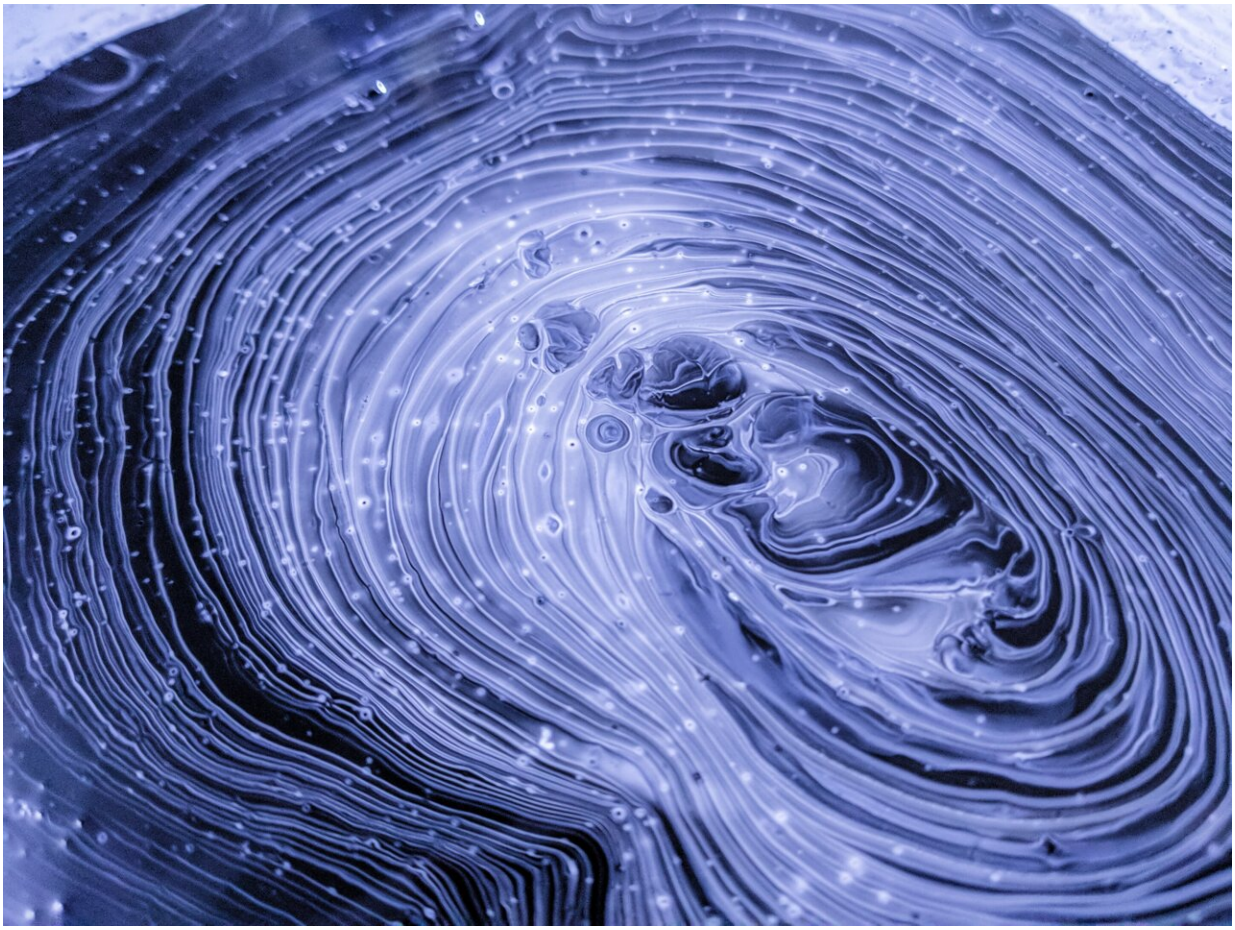
DNS-over-HTTPS: why the web's latest privacy tech is causing an outcry

October 30 2019, by Gareth Tyson and Timm Böttger



Credit: CC0 Public Domain

A new technology promises to make your web browser more private

than ever, keeping your internet activity from prying eyes. But some argue your data won't actually be all that private. And others are worried it could actually help criminals including child abusers to avoid justice. Here's what you need to know about DNS-over-HTTPS (DoH).

What is DNS-over-HTTPS?

Whenever you visit a webpage, your web browser first needs to discover the specific location (or IP address) of the computer server hosting it. It does this using something called the domain name system (DNS), which converts those easy to remember names (such as theconversation.com) into computer-readable addresses (such as 151.101.66.110). Your web browser does this by sending a DNS query for the website you want to visit to a huge global database, and then waits for the IP address to come back as the answer.

This system has worked well since the 1980s but has come under growing scrutiny due to its ability to expose private user information. For example, imagine that your neighbour could monitor your wifi network and see all the DNS queries from your web browser. They would be able to identify the websites you have visited.

This is where DNS-over-HTTPS comes in. It is a new technology that encrypts your DNS queries, so that only the intended recipient can decrypt and read them.

This can be particularly helpful when connecting to an unfamiliar or public wifi network that others may be able to monitor. Yet people have raised concerns, particularly after Firefox announced that they would turn it on by default in the US.

This is because web browsers still need to send their encrypted queries to somebody to decrypt and then answer. At the moment, most web

browsers send their queries to a special server operated by the user's internet service provider. Unfortunately, most of these servers do not yet support DNS-over-HTTPS.

This means people wishing to benefit from the DNS-over-HTTPS encryption must currently send their queries to another "third-party" organisation who does support it.

What are the concerns?

Our recent research surveyed a number of these "third-party" DNS-over-HTTPS providers. Overall, we found DNS-over-HTTPS had a minimal impact on web browsing experience. But we also found the technology was dominated by US-based companies, over whom most governments feel they have little control. And this is where problems start to emerge.

For instance, the UK government is reportedly concerned that DNS-over-HTTPS will limit its ability to monitor the web activities of suspected criminals or block illegal material. And the Internet Watch Foundation, an organisation that reports online child abuse images to internet providers, fears DNS-over-HTTPS may hamper the ability to block access to such material, which involves blocking parts of DNS.

In both cases, there is a worry that these "third-party" DNS-over-HTTPS providers may not be sufficiently responsive to requests for content blocking. Yet these complaint procedures are a regularly used and important part of web governance.

Privacy advocates are also concerned about the ability of these "third-party" providers, such as Google and Cloudflare, to record all the DNS-over-HTTPS queries they receive, further expanding their capacity to monitor the world's internet activity. These concerns have reportedly led the US Congress to begin investigating if DNS-over-HTTPS could result

in anti-competitive misconduct.

Furthermore, experts worry that misleading coverage of DNS-over-HTTPS might even lull people into a false sense of security, highlighting that it still leaves users open to many other privacy attacks.

Where to go from here?

These problems stem in part from the current deployment of DNS-over-HTTPS. For instance, concerns over US dominance may disappear if more domestic providers emerge, and law enforcers may become more comfortable if such providers then confirm they will enact their blocking requests. Meanwhile Firefox has now decided not to make DNS-over-HTTPS the default setting on its browser for UK users.

Fundamentally, this debate does not centre on the arrival of a new technology though. As often is the case, it centres on power, who should have it and who should wield it. For example, who should regulate the web, and who should be able to exploit our data? Even if governments and internet companies come to an agreement over DNS-over-HTTPS, the wider debate will be far from over.

Provided by The Conversation