

Why big ISPs aren't happy about Google's plans for encrypted DNS

reader comments

142 with 77 posters participating

Share this story

When you visit a new website, your computer probably submits a request to the domain name system (DNS) to translate the domain name (like `arstechnica.com`) to an IP address. Currently, most DNS queries are unencrypted, which raises privacy and security concerns. Google and Mozilla are trying to address these concerns by adding support in their browsers for sending DNS queries over the encrypted HTTPS protocol.

But major Internet service providers have cried foul. In a September 19 letter to Congress, Big Cable and other telecom industry groups warned that Google's support for DNS over HTTPS (DOH) "could interfere on a mass scale with critical Internet functions, as well as raise data-competition issues."

On Sunday, the *Wall Street Journal* reported that the House Judiciary Committee is taking these concerns seriously. In a September 13 letter, the Judiciary Committee asked Google for details about its DOH plans—including whether Google plans to use data collected via the new protocol for commercial purposes.

But Google says that these concerns are groundless. Despite

insinuations from telecom companies, Google says, the company has no plans to switch Chrome users to its own DNS servers. And while Google didn't mention it, the company has plenty of ways to monitor users' browsing patterns with or without access to their DNS queries.

The telecom industry letter is confusing because it mashes together two different criticisms of Google's DOH plans. One concern is that switching to encrypted DNS would prevent ISPs and others from spying on their users. The other is that, in the process of enabling DOH, Google will switch millions of users over to Google's own DNS servers, leading to a dangerous concentration of control over DNS.

Understanding the debate is easier if we consider each of these concerns separately.

Google says it isn't planning to switch users to its DNS

Let's start with the second concern: that Google will switch Chrome users to its own DNS servers, giving Google concentrated power over DNS. Google's response here is simple.

"Google has no plans to centralize or change people's DNS providers to Google by default," the company said in an email to Ars Technica. "Any claim that we are trying to become the centralized encrypted DNS provider is inaccurate."

Google laid out its plans in detail in a September 10 blog post. Starting with version 78, Chrome will begin experimenting with the new DOH feature. Under the experiment, Chrome will "check if the user's current DNS provider is among a list of DoH-compatible providers, and upgrade to the equivalent DoH service from the same provider," Google wrote. "If the DNS provider isn't in the list, Chrome will continue to operate as it does today."

One possible reason for confusion on this point is that Mozilla is planning a more aggressive rollout of the technology. The company is planning to gradually shift all of its users to DOH—whether or not their existing DNS provider supports it. The shift will make Cloudflare the default DNS provider for many Firefox users, regardless of the DNS settings of the underlying OS.

Mozilla has more latitude to do this because most surveys show Firefox with single-digit market share—and Firefox isn't a major DNS provider in its own right. So there'd be little basis for antitrust scrutiny if Mozilla shifts its users over to a new DNS provider. The same move could raise antitrust concerns if Google started switching Chrome users over to its own DNS. But Google says it has no plans to do that.

DNS over HTTPS means ISPs can't spy on their users

Enlarge / Google CEO Sundar Pichai.

Simon Dawson/Bloomberg via Getty Images

Telecom companies also raised a second concern that applies even if Google doesn't shift anyone to its own DNS servers. Put simply: the lack of DNS encryption is convenient for ISPs.

ISPs sometimes find it useful to monitor their customers' Internet traffic. For example, queries to malware-associated domains can be a signal that a customer's computer is infected with malware. In some cases, ISPs also modify customers DNS queries in-flight. For example, an easy way to block children from accessing adult materials is with an ISP-level filter that re-writes DNS queries for banned domains. Some public Wi-Fi networks use modified DNS queries as a way to redirect users to a network sign-on page.

Some ISPs also use DNS snooping for more controversial purposes—like ad targeting or policing their networks for copyright infringement.

Widespread adoption of DOH would limit ISPs' ability to both monitor and modify customer queries. It wouldn't necessarily eliminate this ability, since ISPs could still use these techniques for customers who use the ISP's own DNS servers. But if customers switched to third-party DNS servers—either from Google or one of its various competitors—then ISPs would no longer have an easy way to tell which sites customers were accessing.

ISPs could still see which IP addresses a customer had accessed, which would give them some information—this can be an effective way to detect malware infections, for example. But this is a cruder way to monitor Internet traffic. Multiple domains can share a single IP address, and domains can change IP addresses over time. So ISPs would wind up with reduced visibility into their customers' browsing habits.

What would a switch mean?

But a switch to DOH would clearly mean ISPs had less ability to monitor and manipulate their customers' browsing activity. Indeed, for advocates that's the point. They believe users, not their ISPs, should be in charge.

Mozilla, which is pushing DOH more aggressively than Google, has taken steps to avoid creating too much chaos in the process. In July, Mozilla said that it wouldn't enable DOH by default in the UK, where ISPs are planning to use DNS to implement legally mandated porn filtering.

Before enabling DOH, Firefox will check if a computer has parental control software installed. In enterprise settings, Mozilla will try to figure out if a switch to DOH will break corporate Intranet features that depend on using specific DNS servers. Firefox will continue using the existing DNS servers in these cases.

So far, Google is only enabling DOH for a selected number of whitelisted DNS providers, so the switch shouldn't cause too many problems. If the company goes beyond that, we can expect it to take measures similar to those Mozilla has taken.

In any event, it's hard to see a policy problem here. ISPs' ability to eavesdrop on their customers' DNS queries is little more than an historical accident. In recent years, websites across the Internet have adopted SSL encryption for the contents of their sites. The encryption of DNS is the natural next step toward a more secure Internet. It may require some painful adjustments by ISPs, but that hardly seems like a reason for policymakers to block the change.

<https://arstechnica.com/?p=1576941>