

Comcast fights Google's encrypted-DNS plan but promises not to spy on users



Enlarge / A Comcast van in Sunnyvale, California, in November 2018.

Getty Images | Andrei Stanescu

reader comments

123 with 107 posters participating

Share this story

Comcast has gone on the record to say that it does not track its broadband users' Web browsing histories, even though the company is lobbying against a Google plan that could make it harder for ISPs to track their users.

Comcast yesterday released a statement titled "The Facts about Privacy with Comcast's Xfinity Internet Service." Comcast said:

Where you go on the Internet is your business, not ours. As your Internet Service Provider, we do not track the websites you visit or apps you use through your broadband connection. Because we don't track that information, we don't use it to build a profile about you and we have never sold that information to anyone.

Comcast further said that it does not and has never sold "information that identifies who you are to anyone," and the company claims it has never sold location data gathered from Comcast's mobile service. Comcast also said it deletes DNS queries generated by its Internet customers every 24 hours "except in very specific cases where we need to research a security or network performance issue, protect against security threats, or comply with a valid legal request."

Comcast's statement came one day after Motherboard ran an article titled "Comcast Is Lobbying Against Encryption That Could Prevent it From Learning Your Browsing History."

In the article, Motherboard published a lobbying presentation that it says Comcast has been distributing to US lawmakers. The Comcast slide deck claims that a Google/Mozilla plan to send DNS queries over the encrypted HTTPS protocol would "centraliz[e] a majority of worldwide DNS data with Google" and "give one provider control of Internet traffic routing and vast amounts of new data about consumers and competitors." When contacted by Ars, Comcast did not confirm or deny that it is distributing the slide deck to lawmakers.

The broadband industry's major lobby groups have also been complaining to Congress about Google's plan for DNS over HTTPS, or simply DoH. Google has said its plan for the Chrome browser is to "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’s public DNS system is one of six providers on the list, which also includes Cleanbrowsing, Cloudflare, DNS.SB, OpenDNS, and Quad9.

If what Google says is accurate, the company will not switch any Chrome users to Google DNS. If a Chrome user relies on their ISP’s DNS or uses another DNS provider that isn’t on the list, Chrome would make no changes for that user. If a Chrome user is using one of the five non-Google options on the list, Chrome would switch the user to the encrypted version of that provider’s DNS system, not to Google’s.

Mozilla plans a more aggressive rollout of encrypted DNS for Firefox, but Comcast and other ISPs have primarily expressed concerns about Google. Google has said that it “has no plans to centralize or change people’s DNS providers to Google by default” and that “any claim that we are trying to become the centralized encrypted DNS provider is inaccurate.”

ISPs exaggerate scope of Google plan

That hasn’t stopped ISPs from urging Congress to intervene and claiming (apparently falsely) that Google plans to automatically switch DNS requests on Chrome for desktops and Chrome for Android to its own DNS servers. A letter to Congress from lobby groups including NCTA, which represents Comcast, claims that Google is making its own DNS service “the encrypted DNS lookup provider by default” on both Chrome and Android.

Comcast’s presentation for lawmakers claims that Google’s plan means that “ISPs and other enterprises will be precluded from seeing and resolving their users’ DNS queries and will be bypassed in favor of Google’s own DNS resolver, i.e., Google

Public DNS.”

“With close to 70 percent of the browser market and over 80 percent of the mobile operating system market globally, Google/Mozilla’s unilateral move will profoundly remake the Internet to Google’s liking by centralizing DNS data in Google’s hands,” Comcast said.

Comcast further said that “Google’s unilateral imposition of default, *centralized* DNS encryption will harm key components of the Internet” and that “Congress should demand that Google pause and answer key questions.” Here are some of the questions that Comcast says Congress should force Google to answer:

- *How will Google address security concerns that arise from having just a single DNS resolver for a large proportion of US Internet traffic?*
- *Is it good for Google to be the sole source of malware protection for the entire US Internet ecosystem?*
- *Given Google’s market power in the browser and OS market, and because Google is attempting to seize control of DNS data, does this raise competitive concerns?*
- *Will consumer’s [sic] be given a meaningful choice to avoid Google and Mozilla’s DNS services—how will Google explain the risks to customers?*
- *How will Google support parental controls and content filtering? Will such services be provided exclusively by Google and/or those it does business with?*

Comcast’s opposition to Google’s plans could raise concerns that Comcast is tracking its broadband users’ browsing activity. Those same concerns were raised when Comcast and other ISPs lobbied Congress to kill broadband privacy rules in 2017. The federal government’s decision to eliminate privacy rules at the broadband industry’s request means that companies

like Comcast are not prohibited from using customers' browsing histories to sell targeted ads or from sharing customers' browsing histories with third parties.

Comcast defended its privacy practices at the time, saying that it doesn't sell its users' Web browsing histories.

What is Comcast worried about?

But if Comcast isn't tracking its users, why is it so concerned about Google's DNS plans? Comcast's presentation says that Google deploying encrypted DNS would "create challenges for content delivery, content protection, law enforcement, and ISP customer support/troubleshooting" and "undermine network service quality and performance—including 5G."

In a statement to Ars, Comcast said it supports encrypted DNS but that it "want[s] to make sure that it is implemented in a careful, collaborative manner for the benefit of Internet customers to ensure that important parental controls, cybersecurity protections, and network security features are not broken in the process." Comcast said it would support a "collaborative, industry-wide solution that protects everyone," but not "unilateral action" by Google and Mozilla.

Comcast's other statement about its privacy practices doesn't name Google, but the cable company is clearly trying to draw a distinction between the privacy of its own service and the privacy of Google's.

"We've never used [DNS query] data for any sort of marketing or advertising—and we have never sold it to anyone," Comcast said.

Google makes most of its revenue from advertising and collects browsing data in order to target ads at users. But Google says that Google Public DNS is not used to serve ads and that it

doesn't correlate IP addresses or location data with users' personal information.

Comcast runs an advertising business

While Comcast says it doesn't track its users' browsing history, Comcast does sell online ads for "multiple premium, high-traffic online destinations" through its advertising business.

Comcast's website says that it may target online ads based on users' information, though apparently not their browsing histories:

Comcast may sell graphical display, text, and other ads, and deliver promotional offers for its products and services, on the Comcast Web Services and other digital properties. These ads and promotional offers may be based on information that you have provided to Comcast or its affiliates (such as the ZIP code of your Xfinity Internet service address), information about your current subscription or use of Comcast's or its affiliates' products or services, or other generally available information about you.

Comcast also sells targeted ads on its cable TV service.

Since Comcast already operates an advertising platform, it probably wouldn't be difficult for the company to track its broadband users' browsing histories in order to serve targeted ads. (AT&T used to do exactly that.) Comcast may not track browsing activity today, but its lobbying against privacy rules and Google's DNS plans could help Comcast keep its options open.

<https://arstechnica.com/?p=1591629>