User Expectations and Understanding of Encrypted DNS Settings

Alexandra Nisenoff, **Nick Feamster**,
Madeleine A Hoofnagle, Sydney Zink

THE UNIVERSITY OF CHICAGO

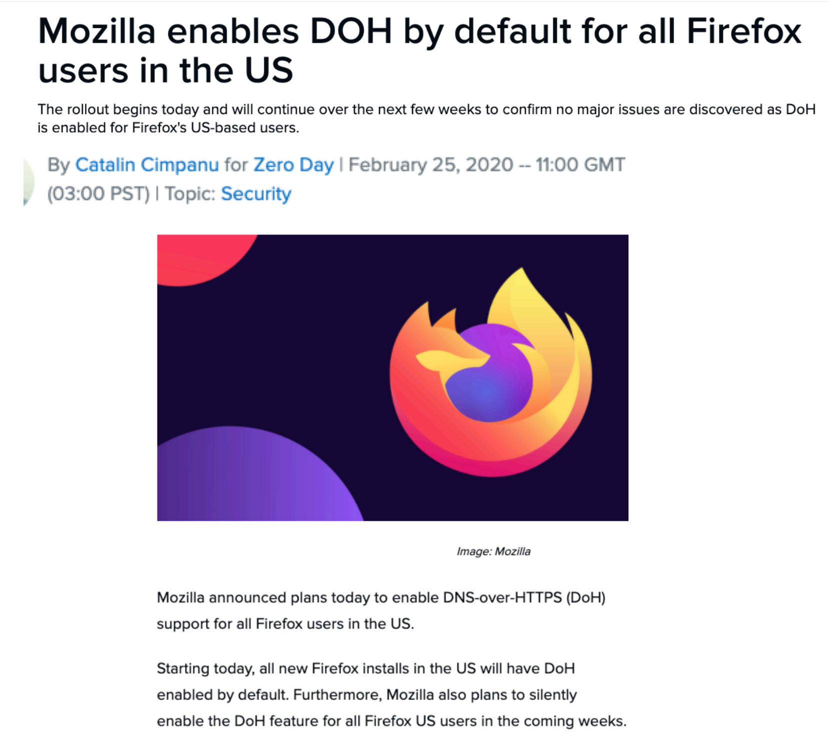
Center for Data and Computing
AT THE UNIVERSITY OF CHICAGO

Northwestern University

Encrypted DNS is Now Often “On by Default”

- Encrypted DNS is being deployed in browsers, operating systems
  - Often it is enabled by default
  - Trusted recursive resolver is also selected by default
  - Chromium: Opportunistic DoH
  - Firefox and Opera: Cloudflare is default TRRs

- **Do users want this?**
- **Do they understand it?**
- **Do they know how to change it?**



Mozilla enables DOH by default for all Firefox users in the US

The rollout begins today and will continue over the next few weeks to confirm no major issues are discovered as DoH is enabled for Firefox's US-based users.

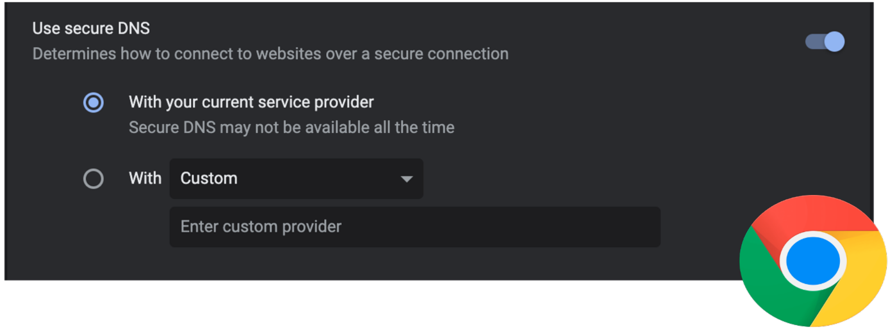
By Catalin Cimpanu for Zero Day | February 25, 2020 -- 11:00 GMT (03:00 PST) | Topic: Security

Image: Mozilla

Mozilla announced plans today to enable DNS-over-HTTPS (DoH) support for all Firefox users in the US.

Starting today, all new Firefox installs in the US will have DoH enabled by default. Furthermore, Mozilla also plans to silently enable the DoH feature for all Firefox US users in the coming weeks.

Enabling DNS-over-HTTPS



Use secure DNS

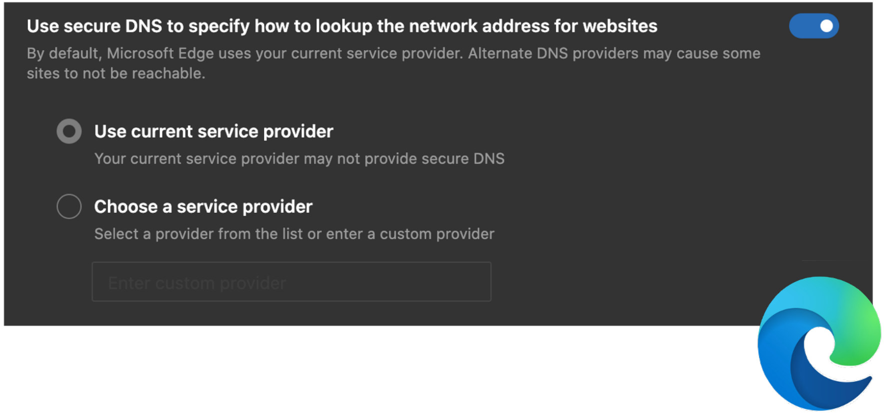
Determines how to connect to websites over a secure connection

● With your current service provider

Secure DNS may not be available all the time

○ With Custom

Enter custom provider



Use secure DNS to specify how to lookup the network address for websites

By default, Microsoft Edge uses your current service provider. Alternate DNS providers may cause some sites to not be reachable.

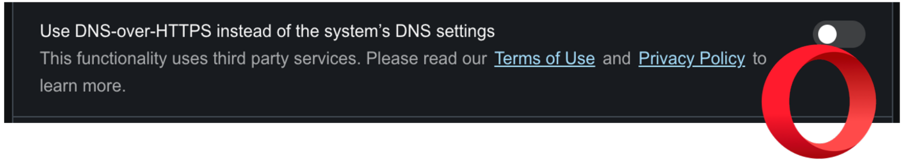
● **Use current service provider**

Your current service provider may not provide secure DNS

○ **Choose a service provider**

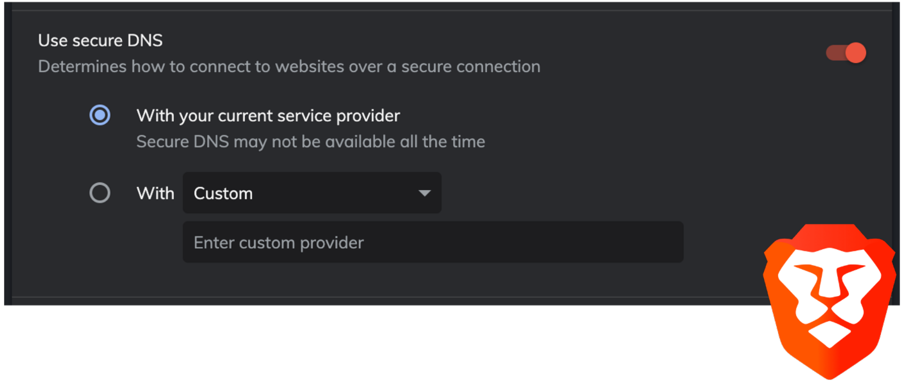
Select a provider from the list or enter a custom provider

Enter custom provider



Use DNS-over-HTTPS instead of the system's DNS settings

This functionality uses third party services. Please read our Terms of Use and Privacy Policy to learn more.



Use secure DNS

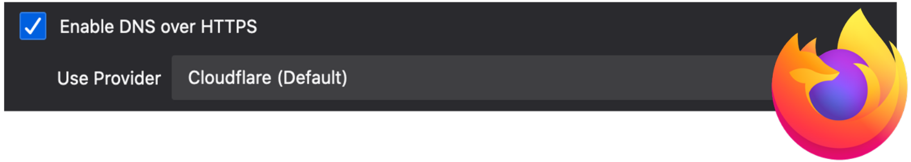
Determines how to connect to websites over a secure connection

● With your current service provider

Secure DNS may not be available all the time

○ With Custom

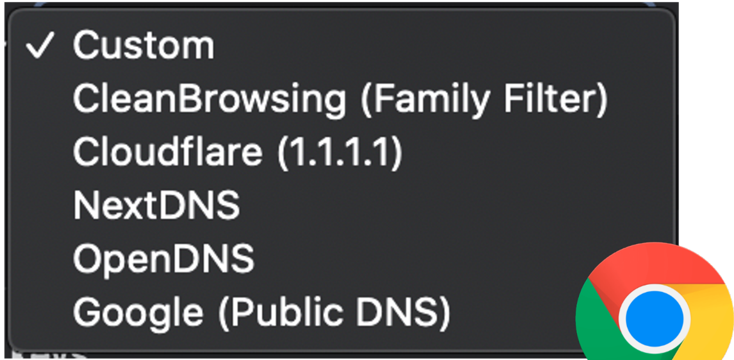
Enter custom provider



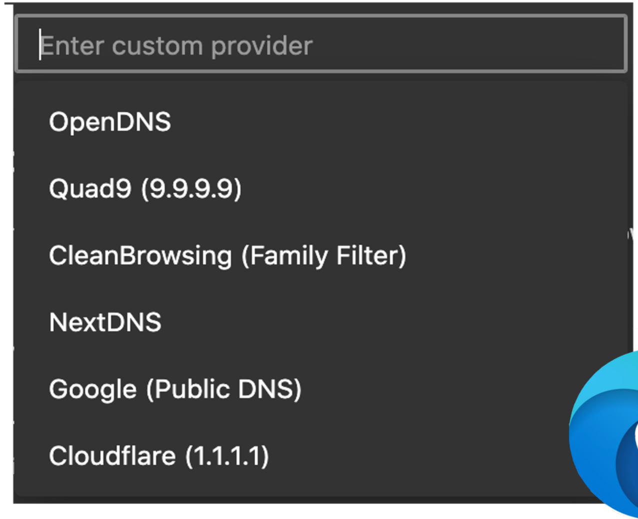
☑ Enable DNS over HTTPS

Use Provider Cloudflare (Default)

Choosing a Trusted Recursive

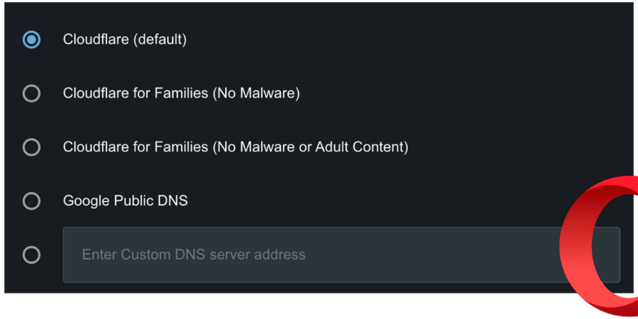


- ✓ Custom
- CleanBrowsing (Family Filter)
- Cloudflare (1.1.1.1)
- NextDNS
- OpenDNS
- Google (Public DNS)

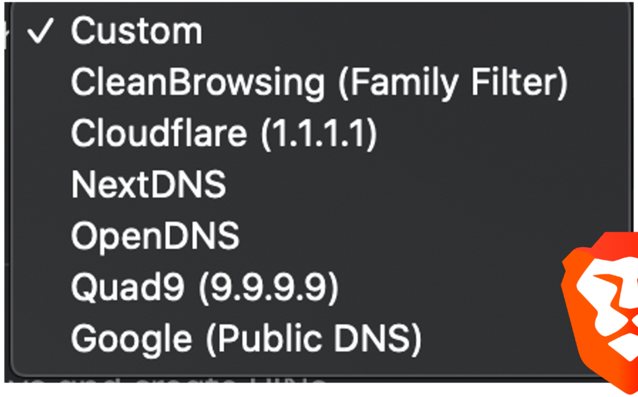


Enter custom provider

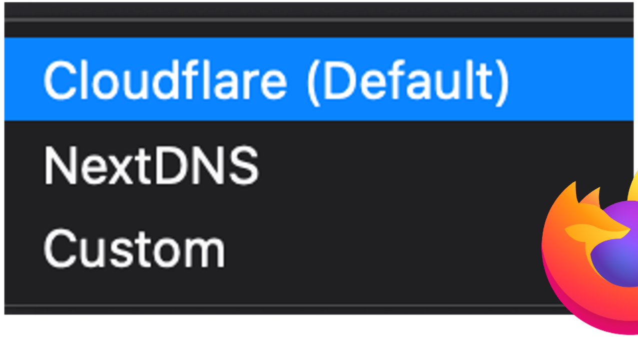
- OpenDNS
- Quad9 (9.9.9.9)
- CleanBrowsing (Family Filter)
- NextDNS
- Google (Public DNS)
- Cloudflare (1.1.1.1)



- ● Cloudflare (default)
- ○ Cloudflare for Families (No Malware)
- ○ Cloudflare for Families (No Malware or Adult Content)
- ○ Google Public DNS
- ○ Enter Custom DNS server address



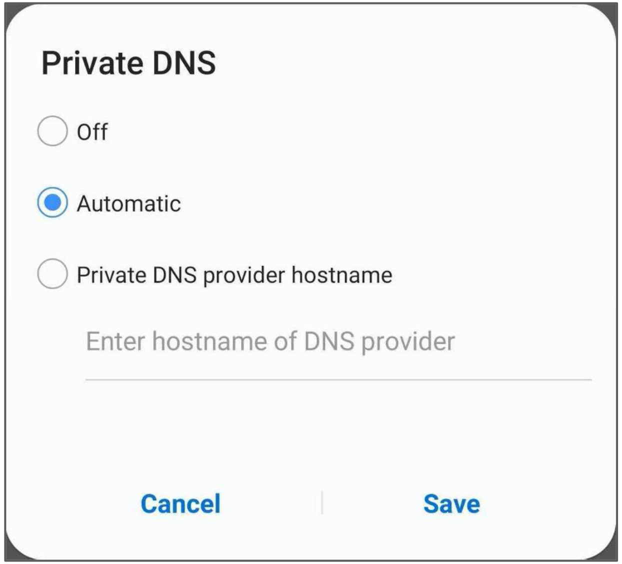
- ✓ Custom
- CleanBrowsing (Family Filter)
- Cloudflare (1.1.1.1)
- NextDNS
- OpenDNS
- Quad9 (9.9.9.9)
- Google (Public DNS)



- Cloudflare (Default)
- NextDNS
- Custom

Pilot Survey: Questions

- Do users **understand** what DNS **setting options** do?
  - **Users have misconceptions about DNS settings**
- How do users **interact** with current DNS setting options?
  - **Users mostly don’t interact with these settings or leave them on their default options**
- **Why** do users choose the settings that they do?
  - **Users stick with default settings** when they lack information
  - **Many thought the defaults were necessary** for their phone to work
- Does being provided with more information on DNS settings change the settings option that users choose?
  - **Some users do change their settings**.
- Do people know about the different DNS resolvers? Do they trust them?
  - People had **limited knowledge** of DNS resolvers
  - **Trust in those resolvers varied** among participants



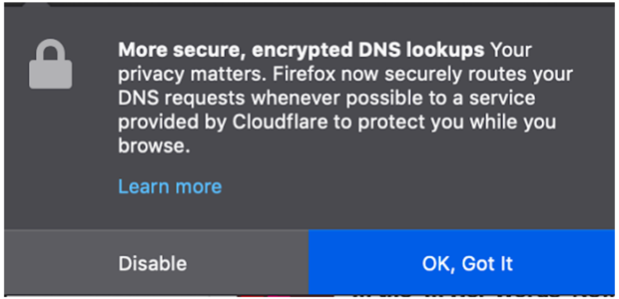
Private DNS

○ Off

● Automatic

○ Private DNS provider hostname

Enter hostname of DNS provider

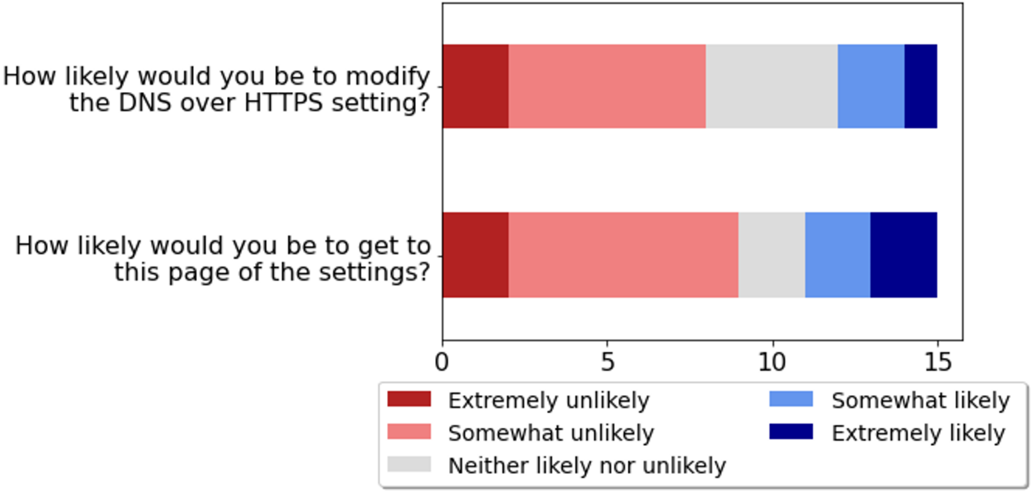


More secure, encrypted DNS lookups Your privacy matters. Firefox now securely routes your DNS requests whenever possible to a service provided by Cloudflare to protect you while you browse.

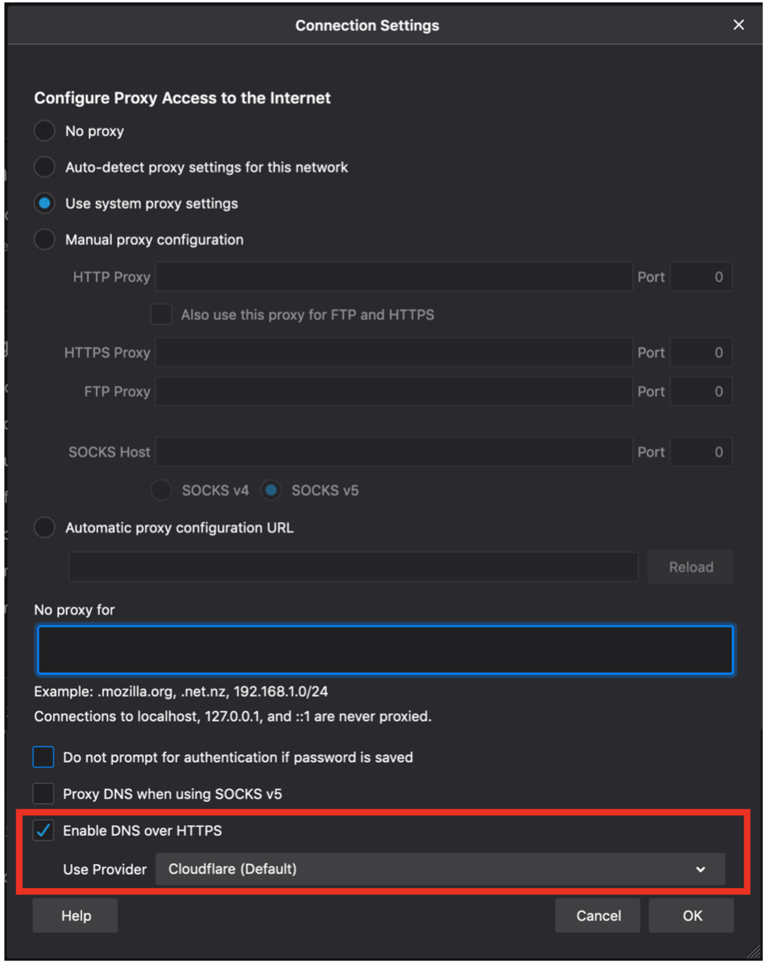
Survey Design (15 participants via Prolific)

- Participants were shown the popup that is displayed to users, after the update that enabled this feature.
  - They were asked which of the two options from the popup they would select and whether they had seen the popup before taking the survey.
  - Participants were shown screen shots of the Firefox settings menus and were asked questions about how likely they would be to modify the setting or be able to find this setting on their own.
- If participants had a phone that supported Private DNS, they were asked to navigate to the Private DNS settings page.
  - If they were able to get to the Private DNS settings page they were asked about their current settings. Users that were not able to navigate to the Private DNS settings page or had a phone that did not support Private DNS were shown images of the Private DNS settings page.
  - All participants were then asked what Private DNS they would choose without any additional information about Private DNS.
- After a brief description of DNS was given and a question to confirm that participants had understood the description, participants were asked what aspects of their DNS traffic they would expect to be protected by Private DNS.
  - Following an explanation of Private DNS, participants were asked multiple-choice and open-ended questions regarding their opinions of this setting. Participants were then presented the original settings options for Private DNS and asked what option they would choose.

Changing Settings in Firefox



User responses to questions about Firefox's DoH settings



Connection Settings

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

● Use system proxy settings

○ Manual proxy configuration

HTTP Proxy Port 0

□ Also use this proxy for FTP and HTTPS

HTTPS Proxy Port 0

FTP Proxy Port 0

SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24

Connections to localhost, 127.0.0.1, and ::1 are never proxied.

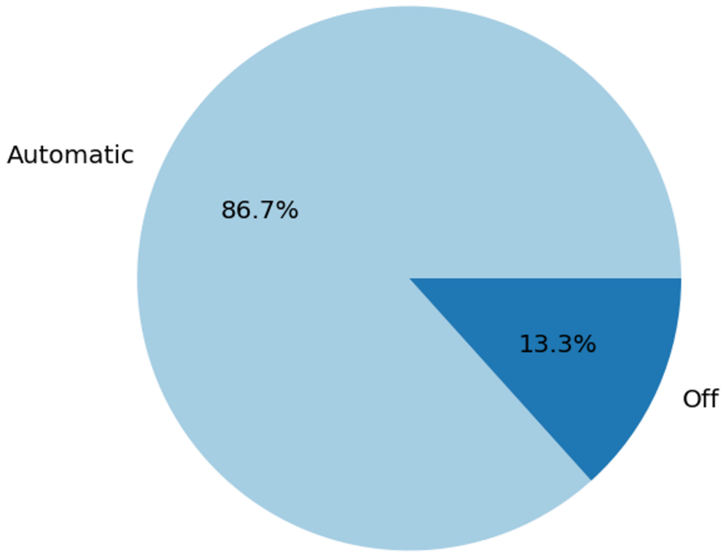
□ Do not prompt for authentication if password is saved

□ Proxy DNS when using SOCKS v5

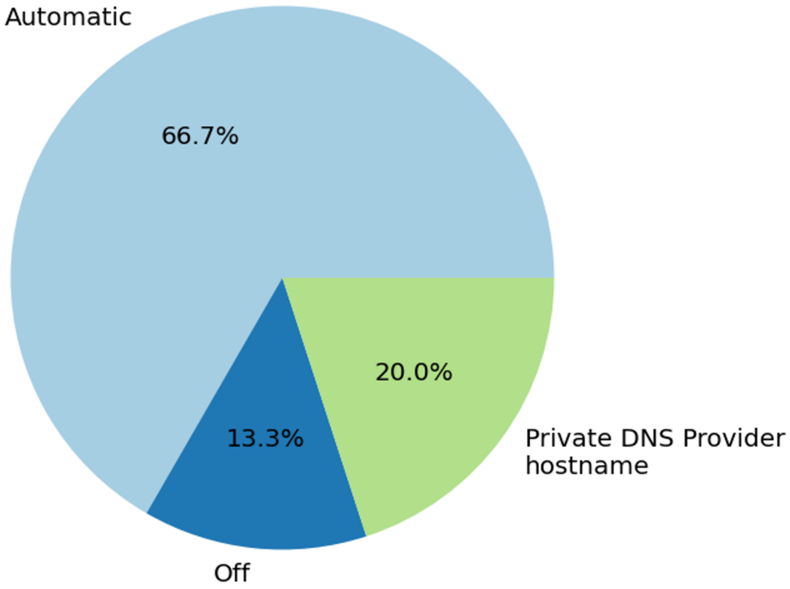
☑ Enable DNS over HTTPS

Use Provider: Cloudflare (Default)

Choices of Encrypted DNS Settings: Automatic or Other?

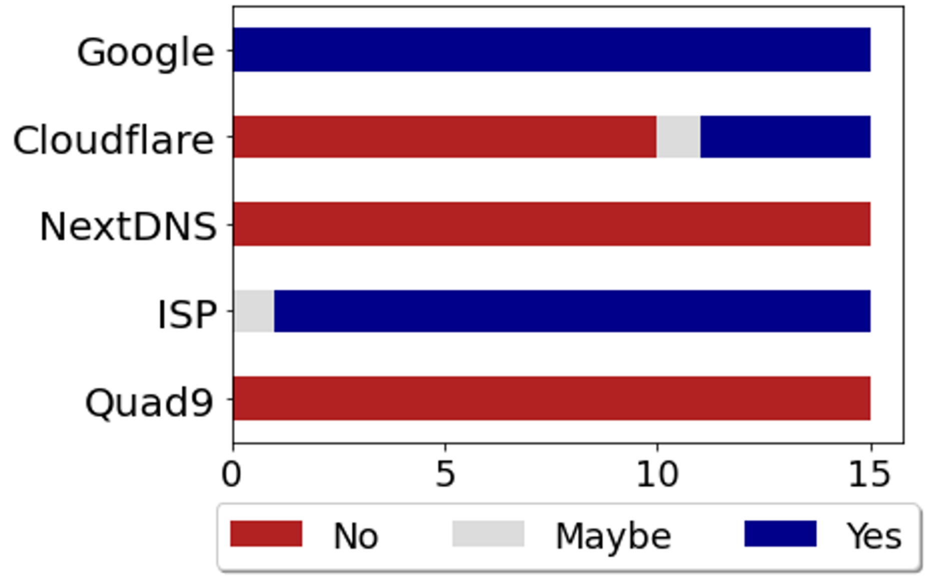


Private DNS setting choice without additional information

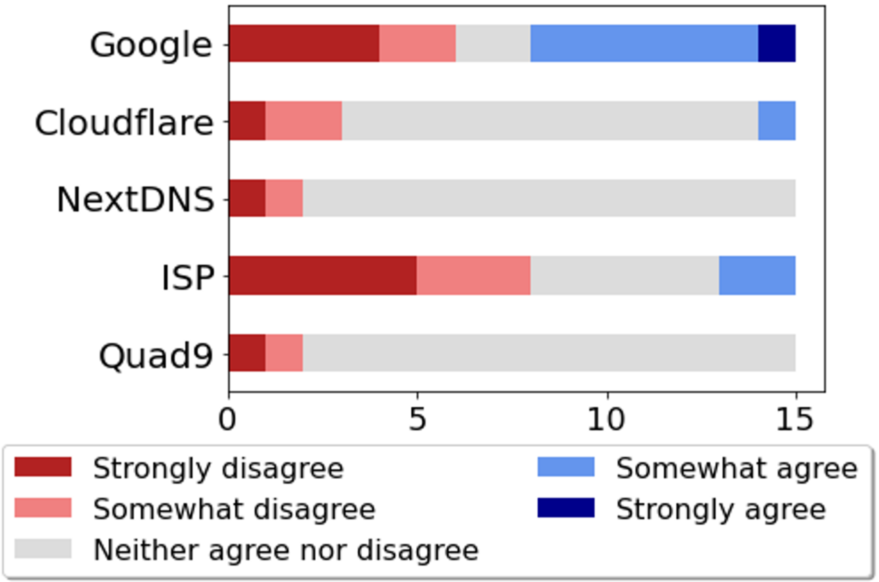


Private DNS setting choice with additional information

Knowledge of and Trust in DNS Providers



If participants had heard of different DNS providers



If participants reported trusting different DNS providers

Summary and Future Directions

- Main Findings
    - Many people stick with default settings options making the choice of default very important
    - People don’t understand the ramifications of selecting different options
    - Being given more information does cause some people to choose a different option
    - There is still a lot of work to do on explaining these settings to users
- Future Directions
    - Larger sample size
    - More extensive interface testing
        - Test newly implemented interfaces
        - Design and test alternative interfaces
        - Have more participants be able to interact with their own settings
    - Understand users’ expectations for each encrypted DNS configuration