Google's Proposed Public DNS Plans

Summary

- The Domain Name System or “DNS” is the **cornerstone of the Internet**. It is the essential “address book” that links textual domain names (www.example.com) to IP addresses (93.184.216.34) associated with websites and other content.

- DNS today operates in a **widely distributed manner**—ensuring the safety and reliability of the Internet— enabling malware protection, parental controls, content filtering, Content Deliver Network (CDN) localization, and others.
- The Internet Engineering Task Force (“IETF”) last year adopted **encryption standards for DNS data**, called DNS over HTTPS (“DoH”) (browser) and DNS over TLS (“DoT”) (mobile OS).
- Many players in the ecosystem have come together to explore an implementation of this standard that would maintain today’s distributed DNS model and an approach that would **respect the multi-stakeholder uses of DNS**.

Summary

- However, Google has announced **unilateral plans** (along with Mozilla, which derives over 90% of its revenue from Google) to activate DoH in its Chrome browser as soon as October. Google also appears poised to activate DoT for devices using its Android mobile operating system in the near future.
- If activated, this feature would by default route all DNS traffic from Chrome and Android users to Google Public DNS, thus **centralizing a majority of worldwide DNS data with Google**.
- This change would mark a **fundamental shift** in the decentralized nature of the Internet's architecture and give one provider control of Internet traffic routing and vast amounts of new data about consumers and competitors.
- The unilateral centralization of DNS raises serious policy issues relating to **cybersecurity**, privacy, antitrust, **national security and law enforcement**, **network performance and service quality (including 5G),** and other areas.

DNS Today

- Today, DNS is provided by a broad array of entities, with millions of DNS providers spread around the globe.
    - ISPs and mobile network operators (MNOs) typically provide DNS to their own customers, and enterprises, schools, and other networks often operate their own DNS solutions.
- This distributed approach is a cornerstone of the distributed model of the Internet. The resulting decentralization and redundancy serves as a key part of the Internet's ultimate resiliency to physical and cyber attack.
- DNS providers have developed and continue to improve on security standards, but always on the basis of broad consensus across the ecosystem and with deployment over time to ensure proper functioning.

DNS Today

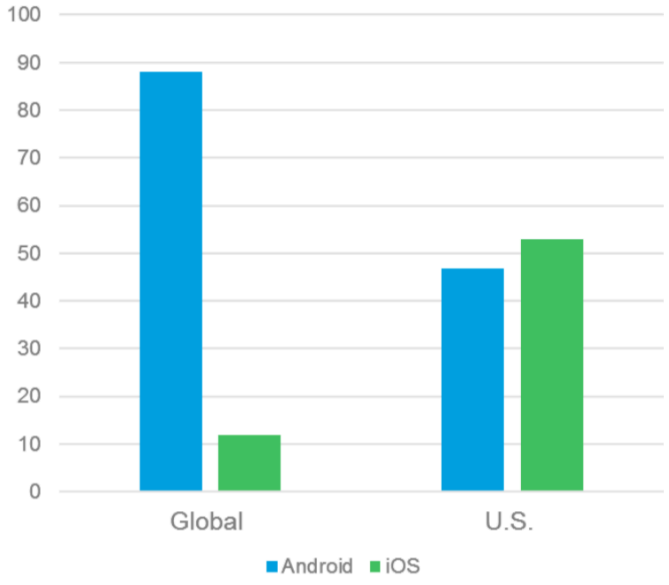
- DNS is used to respond to Internet subscriber requests, but also for other network functions.
  - **Anti-malware tools**, whether provisioned by ISPs or third parties, use DNS query data to block or detect user access to suspect sites.
  - **Parental controls and content filters** from ISPs and third parties likewise rely on DNS query data.
  - **CDN localization for low-latency and resilient delivery of online video** relies on geographic location data contained in a DNS query to select the closest server from which to provision the requested content.
  - **DNS data is available today for law enforcement**, in non-encrypted form, and is also sometimes used for site blocking for law enforcement efforts.
  - **DNS is used for self-service installations**, troubleshooting, and implementation of service plan terms that increase customer choice.

Google's Unilateral Imposition of Default, *Centralized* DNS Encryption Will Harm Key Components of the Internet

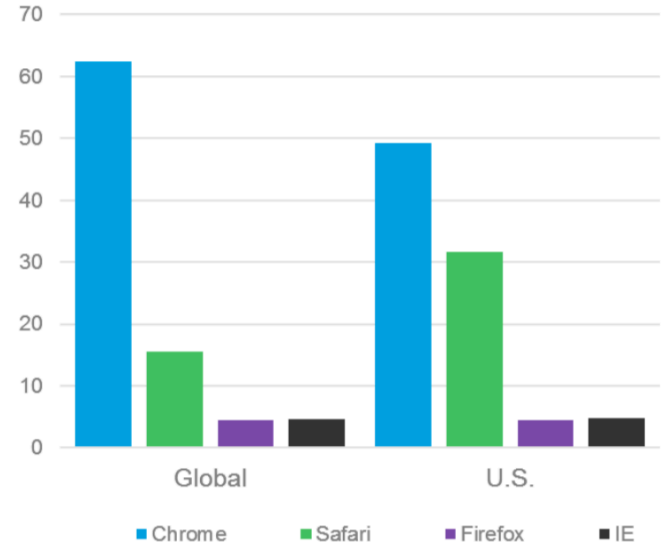
- Recently, Google has announced unilateral plans to implement DoH by default in its Chrome browser *in the very near term*. Implementation in its Android operating system would follow. Mozilla has announced similar plans with respect to Firefox.
- With close to 70% of the browser market and over 80% 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.
- Despite numerous requests and discussions with many others in the ecosystem, Google has been unwilling to slow its course, or fully consider and test the impact and means to ameliorate that impact.
- Congress should take a hard look at the implications for the economy, competition, consumer privacy and service quality, as well as national security and law enforcement.
- Many government entities in the EU—particularly Parliament and law enforcement in the UK—have expressed a high degree of alarm over Google's plan; this has prompted Google and Mozilla to back off in Europe and focus their plans solely on North America (at this time).

Google Is the Dominant Browser and Mobile OS Provider

Mobile OS Market Share



Browser Market Share



[1] With Chrome and Firefox, Google and Mozilla together control approximately 70% of the global browser market share and approximately 55% of the U.S. market.

Google's Plans Will Cause Radical Disruption

- If Google encrypts and centralizes DNS, 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.
- Bypassing ISPs and other enterprises will:
  - Undermine Internet security;
  - Provide Google with a vast new storehouse of both user and competitor data;
  - Concentrate the provision of DNS resolution and decryption in the hands of one company;
  - Disrupt existing parental controls and content filtering;
  - Create challenges for content delivery, content protection, law enforcement, and ISP customer support/troubleshooting; and
  - Undermine network service quality and performance—including 5G.

- Why is Google in such a rush?

Significant Cybersecurity and National Security Risks

- As noted, DNS resolution today is done by numerous ISPs and MNOs around the world, creating significant redundancy and ensuring no single point of failure.
- By switching its default setting, Google will centralize DNS resolution in the hands of one dominant firm. This will create a single point of failure, and a single group of employees and backend systems that can be targeted—making DNS resolution more vulnerable to cyberattacks and putting networks worldwide at greater risk.
- Google's implementation also appears likely to break the tools that networks currently use to fight cyberattacks and protect consumers. When these tools are disrupted, malware, bots and other attacks can proliferate more broadly across the Internet.
    - In addition, critical innovation in this area will be reduced if Google is the only firm able to provision security tools.

Privacy Risks Increase as a Single Firm Amasses More Consumer Data

- Today, DNS operations are completely decentralized. An ISP can only see users' DNS data on its own network and cannot link this up with data from usage on other networks.
- Centralized DNS will give Google unprecedented visibility into what users are doing and what websites or apps they are visiting on the Internet *across* networks and devices *around the world.*
    - In other words, centralized DNS encryption will allow Google to enhance its vast data storehouse and create even more comprehensive user profiles.
- Thus, while cloaked as enhancing user privacy, Google's DNS encryption will in fact vastly expand Google's control over and use of customer data, and will result in the complete commercialization of DNS data for Google's own ends.

Antitrust and Competition Concerns

- Google has a dominant position, approaching monopoly, in the browser and mobile OS markets.
- Google already has unrivaled access to a vast amount of data about consumers through its dominance of a variety of Internet business lines, including:
  - Search
  - Advertising and ad tech
  - Browsers
  - Mobile operating systems
  - Online video platforms (YouTube)
  - Email, maps, etc.
- Google's unilateral switch to centralized DNS will add another huge source of data to Google's enormous data pool, which it already aggressively monetizes.
- Moreover, Google will be uniquely situated to use this DNS data to advantage its adjacent businesses and undermine competitors in those segments, including:
  - Competitive DNS providers
  - CDN providers
  - Advertising
  - Internet of Things providers
  - Online video rivals

Law Enforcement Efforts May Be Compromised

- Some ecosystem players have used encryption to foil legitimate law enforcement efforts. Centralized DNS encryption can be designed to do the same.
- Today, ISPs have well-established procedures to comply with legitimate law enforcement inquiries relating to, among other things, DNS.
    - Google's DNS encryption approach will result in increased complexity, costs, and delay for law enforcement.
- Further, ISPs could not, if directed by law enforcement, block access to sites using DNS data. In Europe, where certain laws direct ISPs to block child pornography, this has emerged as a very significant law enforcement concern.

CDN Localization Will Likely Suffer and Backbone Costs Will Rise

- A Content Delivery Network ("CDN") is a system of distributed servers that delivers Internet content to an end-user based on the user's geographic location.
    - CDNs help content publishers ensure quick access to content and high performance by distributing data from servers that are geographically closer to end-users. This localization dramatically reduces latency and improves the consumer experience and the performance of online services, particularly high bandwidth services like online video.
    - CDNs depend in part on DNS data in order to provide this critical service.
- Without localized DNS-based data, CDNs will not be able to deliver content along the optimal, shortest path to consumers.
    - Delivery costs will increase as content is dropped off at remote sites and delivered using expensive Internet backbone resources—ultimately resulting in higher costs to consumers. Content performance will also be degraded.
- CDNs will be required to go through Google to address the issue, giving Google the power to determine how CDNs work; only Google's CDN services—or those that it supports with localization data—will reliably work. Google's own YouTube, YouTube TV, and other online services will have the only assurance of low latency, localized delivery.

Wireless Performance, Including 5G, Will Be Undermined

- Low latency is a key benefit of 5G and is critical to enabling use cases such as:
  - Autonomous vehicles
  - Telemedicine and medical devices
  - Smart cities and other public safety initiatives
- These latency benefits require storing content closer to users (“the edge”).
- If Google and Mozilla implement DoH by default, content queried through their browsers or via Android OS could be cached much further away from the user, undermining the low latency benefits 5G has the potential to deliver.
- Overall 5G performance could be undermined because of strain on the Internet backbone caused by the need to transport content over longer distances.
- Gives Google control over optimization of services that compete with its own.
- DoH by default would break and require redesign of internal services and features that rely on DNS (e.g., WiFi authentication, MMS, visual voicemail, load balancing, parental controls, data plan management).

Parental Controls/Content Filtering May Be Disabled

- Today, ISPs and other firms offer parental controls and content filtering solutions by using DNS to block access to “blacklisted” websites and content.
- Default switching to centralized encrypted DNS may disable these critical services and make it impossible for ISPs or others to offer these services.
  - Parents who rely on their ISPs to provide these services (or who buy them from third parties) will see them automatically undermined any time their child uses Chrome or an Android mobile device, or the Chromebook their child got from their school.
  - Schools and libraries will be at risk of non-compliance with E-Rate funding requirements that require content filtering.
  - Various enterprises that use content filtering to create safe workplaces will have more difficulty doing so.
- Only Google will be able to offer all of these services with no degradation.
  - Parents, schools, and libraries will be forced to switch to Google’s services to ensure required content filtering services work properly even though they already had purchased the services elsewhere.
  - With this elimination of competition, high quality, innovative services may not be developed or may cease to be offered.

ISPs and Other Enterprise Services May Be Disrupted or Broken

- Large enterprises, including government agencies, that offer their own internal “split DNS” to support large intranets and rely on DNS for filtering, malware detection, and other protective measures may no longer be able to do so if they use Google for browser or mobile OS purposes.
  - In theory, these enterprises could preclude the use of Google—but this type of command and control over network use is far from the norm; further, many enterprises support users bringing their own devices, which are not subject to such control.
  - Default centralized DNS will expose their internal DNS data to Google for resolution.
  - This may be a competitive issue for some enterprises that compete with Google; for others (government contractors, for example) it may be a security issue to have the names of internal systems exposed in this way.
- Default switching also will likely break ISP efforts to support customer self-installations and to provide diagnostic support for Internet connectivity issues.

Congress Should Demand that Google Pause and Answer Key Questions

- How will Google address security concerns that arise from having just a single DNS resolver for a large proportion of U.S. Internet traffic? Is it good for Google to be the sole source of malware protection for the entire U.S. Internet ecosystem?
- Has Google tested whether this will result in more malware, cyber threats and higher latency online video delivery?
- Is Google planning to use DNS data for any purpose other than DNS resolution? Will Google engage in commercial applications of DNS (including enrichment of internal Google commercial databases)?
- Google competes in the OTT video marketplace and several other online markets (music, voice assistants, etc.). If Google provides centralized DNS in its mobile operating system, Google will have extensive oversight and insight into the use and functionality of the OTT apps of its competitors in this linear space. How will Google protect against anticompetitive uses of the data it receives concerning its competitors' services? Are there structural protections in place? How would this be enforced?
- 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 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?
- How can CDNs localize content delivery after Google's implementation in a way that ensures that Google does not become the sole provider of CDN? How will Google's implementation affect mobile operators that also rely on localization to provide low-latency applications.
- Can enterprises or the government avoid exposing their internal DNA/data/Internet queries to Google while still using Chrome or Android?