Briefing

The Impact of the Private Relay Service on Network Operators and Internet Service Providers

Andrew Campling
10th September 2021

419.Consulting

(This page is intentionally blank)

Cover image by Gerd Altmann from Pixabay

The Impact of the Private Relay Service on Network Operators and Internet Service Providers

1. Foreword

A series of technologies are currently being developed that are intended to improve the privacy of the Internet by updating or extending some of the core standards that underpin its operation. These changes are being led within various working groups of the Internet Engineering Task Force (IETF), leveraging the expertise of developers drawn from across the industry.

In some cases, these industry initiatives are augmented by developments led by individual companies; Private relay is an example of the latter. The Private Relay service has been developed by Apple as an extension of its iCloud+ service for devices running the iOS 15, iPadOS 15 and macOS Monterey operating systems. It was announced at Apple's annual developer conference in June 2021[1], with more technical detail made available during a discussion with one of the senior engineers a few weeks later[2].

A recent roundtable considered the implications of Private Relay for network operators, Internet Service Providers (ISPs) and others. The purpose of the discussion was to evaluate the impact of Private Relay and identify whether these caused any unintended consequences that would have operational or other adverse impacts.

This document summarises elements of the roundtable to highlight some of the key impacts of Private Relay as well as the steps that need to be taken in order to mitigate the negative consequences of its introduction, in both the immediate- and longer-term. The conclusions and recommendations are based on the content of the discussion, augmented where necessary with additional detail whilst retaining the spirit of the points raised during the roundtable.

For those interested in more information, detailed notes from the roundtable are available separately[3].

[1] See https://developer.apple.com/videos/play/wwdc2021/10096/

[2] See https://419.consulting/encrypted-dns/f/icloud-private-relay

[3] See https://419.consulting/private-relay

2. What are the Likely Impacts of Private Relay?

2.1 Introduction

As noted in the foreword, a recent roundtable looked in detail at Private Relay, primarily from the perspective of network operators and ISPs. The roundtable brought together technologists and others to discuss the likely operational impacts of Private Relay and to consider some of the broader issues raised by the introduction of the service.

The experts concluded that the introduction of Private Relay is likely to cause some operational challenges to ISPs. They also raised compliance and identified potential anti-trust issues that may need attention by regulators and legislators.

2.2 Operational Impacts

Quality of Service and Network Resilience

Any scenario where significant traffic volumes are routed over Private Relay may cause issues for ISPs as they will not have full visibility of traffic that is being carried over their networks. This may affect congestion management and peering optimisation activities undertaken by the ISPs. In addition, connectivity to some sites and services may either become slower or cease working.

More significantly, the quality of service (QoS) measurement methodologies developed under European regulations envisage measurement of functions such as DNS, access to audio/video services, web browsing and other capabilities. ISPs will not be able to comply with any QoS parameters where the traffic is being routed by the Private Relay Service.

Network Costs

When Private Relay is enabled and the egress IP address is not an ISP IP address, the edge content cache that is chosen will never be a CDN cache node embedded in the ISP network; it will instead be a public one. This in turn means that much of the financial and operational investment deploying CDN capacity deep within ISP networks will be unused and content served off-net instead, leading both to increased latency and congestion, as well as to increased off-net costs.

Content Blocking and Filtering

Content blocking and filtering are used by network operators and ISPs for several reasons including:

- In response to court orders blocking access to illegal content such as child sexual abuse material (CSAM)
- To block access to malicious content
- To provide optional filtering capabilities that enable users to block access to certain categories of content, for example in the form of parental controls.

These facilities may not function correctly if Private Relay is enabled[4]. In terms of blocking access to illegal content, legislators and regulators may need to amend existing instruments if they wish to bring Private Relay into scope.

"Zero-Rating" of Content

In consumer markets, both fixed and mobile networks may offer light users packages with data caps at reduced cost, the trade-off being that any data that is consumed over the cap can be relatively expensive. An ISP may opt to allow the customers of these packages access to certain content without it counting towards the data cap.

Zero-rated content may include:

- So-called "public good" material (for example, content related to public health or education)
- Certain premium content (for example sports, films or other entertainment-related material).

[4] DNS-based content filtering will currently continue to function if the device owner or user has specified a preferred DNS provider that supports this functionality as Private Relay does not currently override this setting,

The ability to zero-rate content is lost if the ISP has no visibility of the website that a user is accessing. Users may experience unexpected increases in their bills if they do not realise that content that they were previously able to access freely is now impacting their data allowance.

2.3 Compliance Impacts

Lawful Interception

In some markets, network operators and/or ISPs will have obligations relating to lawful interception of activity undertaken by their users. In terms of voice calls, whether over a mobile network or wi-fi, lawful interception abilities are not affected. However, any access to content, for example by the Safari web browser, is encrypted under Private Relay and so the ISP is unable to help with lawful interception; law enforcement agencies will need to contact Apple to undertake these obligations.

Data Retention and Disclosure

Network operators and/or ISPs may also have obligations concerning data retention and disclosure. As with lawful interception, the ability of network operators or ISPs to fulfil data retention or disclosure obligations is mixed. Voice calls over mobile networks or wi-fi are not impacted by Private Relay and so operators can continue to meet any obligations. However, where a user accesses content, the operator can only show a connection to Apple has been made and not the content that was accessed so law enforcement agencies will need assistance from Apple in order to map access to content to an operator.

Copyright Infringement

There may be issues in jurisdictions where ISPs are no longer able to meet the requirements of court-mandated blocking of access to copyright-infringing material and sites. This may require the scope of court orders and regulatory instruments to be expanded to include Apple to maintain their effectiveness.

3. What are the Antitrust Considerations Relating to Private Relay?

3.1 Possible Competitive Advantage Gained by Participating Vendors

The partners involved with Apple in the delivery of Private Relay, currently believed to include Akamai, Fastly and Cloudflare, may benefit from the knowledge of sites being accessed through the service. This knowledge could provide extremely useful intelligence and analytics for their wider business operations, gaining significant market advantage.

In addition, to optimize performance, Content providers will have an incentive to host their content with the Content Delivery Network (CDN) providers that partner with Apple to deliver the Private Relay service. This may in turn lead to further market distortions.

3.2 Centralisation and Control

Roundtable participants raised concerns about centralisation and control caused by the introduction of Private Relay - “overnight Apple will become the largest ISP in the world”. They noted that its introduction represents a major change in the way that the Internet works. From an architectural perspective, it turns the Internet into a hub-and-spoke rather than mesh network, placing Apple in the centre of a high percentage of transactions.

With Apple being in the path of much of the network traffic emanating from iOS, iPadOS and macOS devices, it effectively becomes the largest ISP on the planet. This may in turn have implications for peering arrangements, impacting both on which parties pay for interconnects and where they have to interconnect. By having control over so much traffic, Apple may gain dominant power, or at least significant market power, in many markets, giving it the ability to dictate terms to ISPs.

3.3 Stifling Debate

An additional issue that came to light during the roundtable was the willingness or otherwise of ISPs and others in the Internet ecosystem to publicly criticize Apple. The suggestion made was that the market dominance of Apple deters companies from going on-record with concerns, a problem that is compounded by the partnerships that Apple has in place with organisations across the ecosystem.

4. Conclusions

The primary conclusions that can be drawn from the analysis of the implications of the deployment of Private Relay are as follows:

1. Network operators and ISPs have concerns relating to quality of service, resilience and costs. They have also identified issues relating to both the filtering and zero-rating of content.
2. Compliance issues have also been raised concerning lawful interception, data retention and disclosure and stopping access to copyright-infringing sites.
3. From an anti-trust perspective, there are concerns about the possible competitive advantage that Apple's partners in the Private Relay service may gain, as well as more fundamental concerns relating to the way that the service changes the operation of the Internet and the control that this gives to Apple.
4. Finally, Apple's dominant position in the market appears to deter other participants from publicly questioning its actions.

All of the above points highlight the need for regulators and legislators to understand the Private Relay service in more detail to identify whether any changes in existing measures are required. For example, modifications to those measures may be needed to bring Apple and Private Relay into scope alongside network operators and ISPs.

The potential antitrust issues also need to be investigated and, if necessary, addressed. In particular, competition authorities need to understand the dominant market position of Apple and take this into account when seeking input from others as there may be a reluctance to comment publicly.

419.Consulting