Briefing

Notes From A Roundtable Discussion About Apple's Private Relay Service

Andrew Campling

7th September 2021

419.Consulting

(This page is intentionally blank)

Notes From A Roundtable Discussion About Apple's Private Relay Service

1. Foreword

The Private Relay service is being 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].

The following notes were taken during a discussion about Private Relay. It covered the implications of Private Relay for network operators, Internet Service Providers and others. The discussion was held under the Chatham House Rule[3] and the comments do not necessarily reflect the views of the author.

The notes from the discussion are in italics, complemented by clarifications added post-meeting in the form of footnotes in plain text. The headings have been added to improve readability, with some text highlighted to draw attention to particular issues or conclusions drawn by the participants.

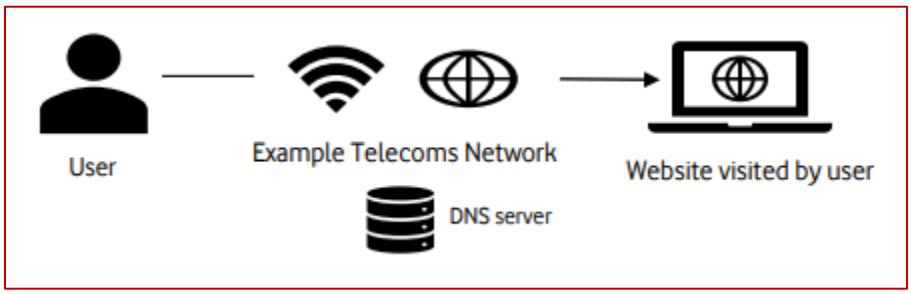
[1] See https://developer.apple.com/videos/play/wwdc2021/10096/
[2] See https://419.consulting/encrypted-dns/f/icloud-private-relay
[3] See https://www.chathamhouse.org/about-us/chatham-house-rule

2. Introductory Presentation

The roundtable began with a presentation to describe how Apple's recently announced Private Relay service functions and to highlight some of the challenges that this may pose. The following text summarises the presentation, with representations of the slides included as Annex A.

How Consumers Access the Internet Today

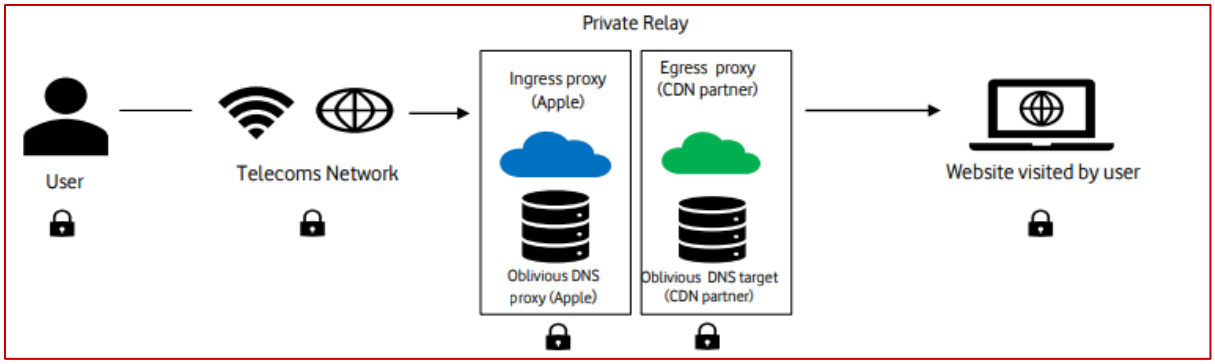
The presentation started with a brief summary of the way that the Internet currently works, highlighting how the Domain Name Service (DNS) is used to translate hostnames or URLs (for example, www.example.com) into the associated Internet Protocol (IP) addresses that allow computers to locate the required content.



In many cases (the majority in many markets), the DNS service is provided by the Internet Service Provider (ISP), typically using a cleartext protocol, although the use of encrypted DNS protocols is becoming more common. The ISPs are able to meet regulatory requirements such as blocking of access to unlawful content or to comply with security obligations.

How Access to the Internet Works with Private Relay

With Private Relay, additional options become available for those users with Apple devices that subscribe to the iCloud+ service. In such cases, selected traffic is encrypted by the device (for example, an iPhone or Mac computer), and then sent to an 'ingress' proxy managed by Apple. It is then forwarded to an 'egress' proxy managed by one of Apple's 3rd party partners. NB Over time, Apple may extend the hosting of ingress proxies to other parties, albeit with the software provided by Apple.



The proxies allocate random IP addresses to users so that websites cannot track users based on their IP address. Neither proxy knows the user's IP address and the website they are visiting meaning that neither websites, Apple nor the CDN partners can track user activity based on their actual IP address.

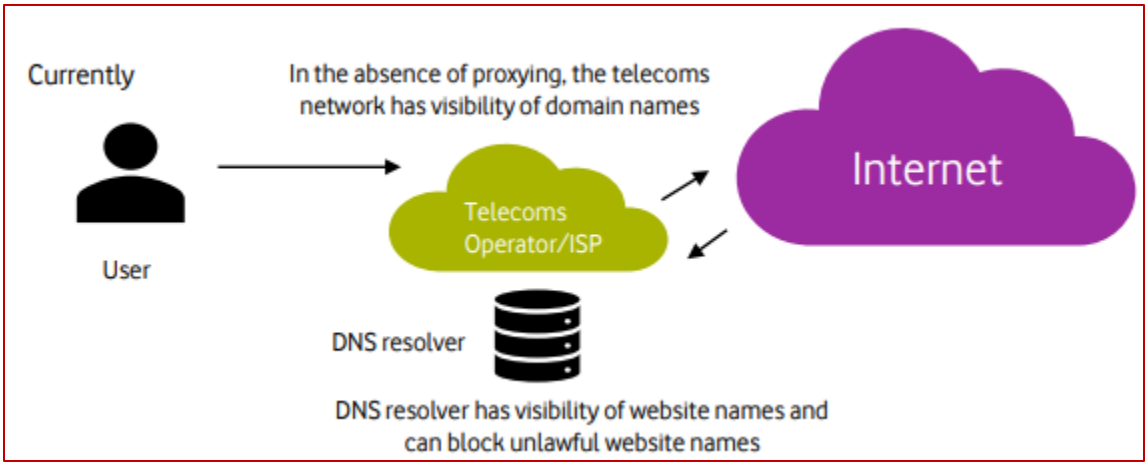
For all iCloud+ customers, the DNS service provided by the ISP is bypassed[4]. They are replaced by DNS nodes provided by Apple and their partner which encrypts and anonymises the domain name resolution requests. This applies not only to browser DNS requests but to all interactions, including those undertaken by other applications, that generate traffic between the user and the Internet.

The process of using ingress and egress proxies is called Oblivious. The protocol used to encrypt DNS traffic that is transmitted in this manner is called Oblivious DNS-over-HTTPS or ODoH[5].

The Implications of Private Relay for Blocking of Unlawful Content and Access to Public Good Websites

In some markets, DNS services block access to websites by removing its name from DNS servers, for example in response to a court order to block access to copyright-infringing material or child sexual abuse material (CSAM). In addition, the DNS operator can undertake content filtering based on the website name (for example, to block access to particular categories of content at the request of a parent or to block access to malicious content).

[4] Unless the user / device owner has specified otherwise or the network operator has disabled private relay; in the latter case, the user will be made aware that the service has been blocked by the network.
[5] See https://datatracker.ietf.org/doc/html/draft-pauly-dprive-oblivious-doh

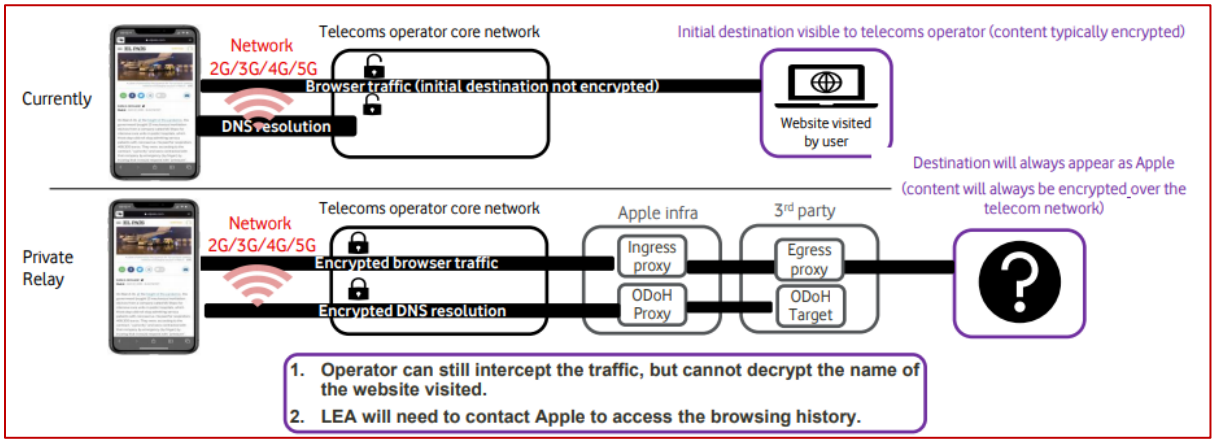


ISPs can also use the DNS service to provide access to "public good" content (for example, that related to health or education) without affecting any data caps that a user may have, effectively "zero rating" the content in question.

These abilities are all lost if the ISP has no visibility of the website being accessed. Any such requirements would then have to be undertaken by Apple or its partner(s), although they would not be able to zero rate access to content as this has to be undertaken by the ISP.

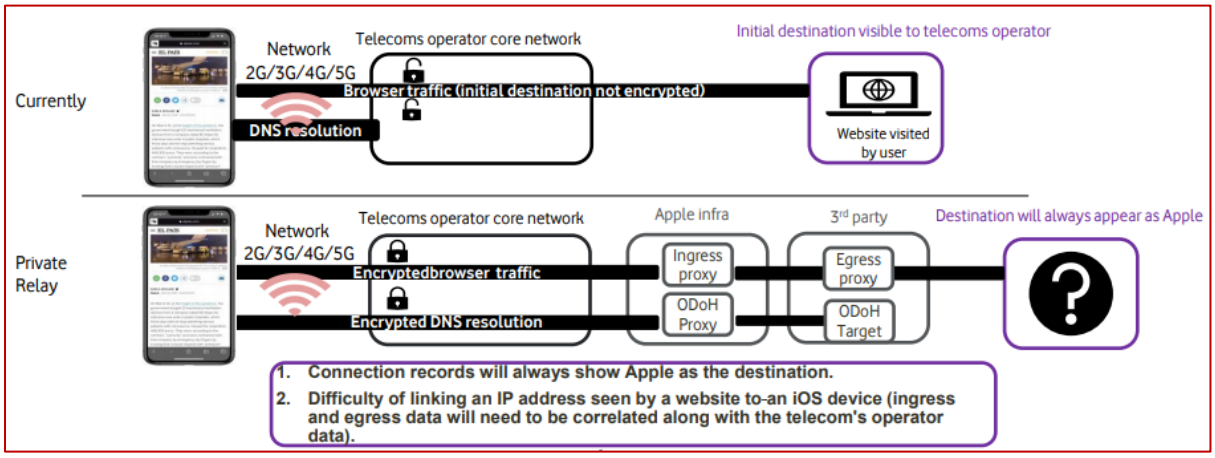
The Implications of Private Relay for Lawful Interception

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, the 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.***



The Implications of Private Relay for Data Retention and Disclosure Obligations

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.***



Note: When content on Apple devices is routed through a MASQUE[6] tunnel, DNS resolution also occurs through that route, with ODoH used as a fallback option where the MASQUE tunnel isn't set up.

The Implications of Private Relay for Meeting Quality of Service Requirements and Achieving 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.*

[6] See https://www.rfc-editor.org/rfc/internet-drafts/draft-schinazi-masque-protocol-03.html

More significantly, quality of service (QoS) measurement methodologies developed under European regulation envisages application-specific 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.***

Thoughts About the Presentation Content

There was broad agreement from participants in the roundtable that the presentation outlined the immediate implications of Private Relay that they had identified.

3. Initial Views

User Experience

Initial analysis suggests that the effects of Private Relay that will be relevant from the perspective of a typical user are the zero rating of traffic as well as general traffic optimization of, for example, video feeds for streaming services depending on resolution etc. Other services affected by Private Relay include edge computing, network identification, network-based malware blocking and parental controls (the participants noted during the discussion that this is not an exhaustive list).

The built-in anonymisation functionality, where the IP address of the user's equipment is replaced with a temporary address can have implications for the the user experience. For example, websites that have restrictions based on IP address may bar access or require users to complete a capcha-based filtering process before access is allowed if a different IP address is being used from that supplied when the user first registered with the site.

Use of Private Relay can be over-ruled on a given device if the owning entity (for enterprise-owned devices) or user has already set preferences to use, for example, a particular DNS resolver. In addition, Private Relay can be disabled selectively, for example at the network level, for an entire device on all services, just for the Safari browser or just for the email application. ***Enterprises generally seem unaware of the existence of Private Relay at present, so will not know that they need to block the service if they wish to continue to enforce enterprise policies****.*

At the time of the roundtable (late July), Private Relay had moved from default on to default off in the latest iOS developer beta software (v4), whereas it is default on in the current public beta software (v3). It is unclear which setting Apple is planning to use for the final version of the software.

If the Private Relay service is launched with all iCloud+ customers opted in and with the service enabled (ie default on), it could have a range of unintended consequences. *For example, sites operated by banks and others that are checking for fraudulent patterns of behaviour (for example, to identify the IP address of devices as part of user validation) may object to redirected and/or reallocated IP addresses.*

Rising 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 offnet instead, leading both to increased latency and congestion, as well as to increased offnet costs.***

4. Antitrust Concerns

Possible Competitive Advantage Gained by Participating Vendors

The egress IP addresses are published and suggest that Akamai, Fastly and Cloudflare are the current CDN operators that are supporting the service. By being involved in Private Relay, these providers will benefit from knowledge of sites being accessed through the service which could provide extremely useful intelligence and analytics for their wider business operations. Egress providers therefore gain significant market advantage.

Content providers will have an incentive to host their content with the CDN providers that operate the Private Relay egress proxies. This may in turn lead to market distortions.

Centralisation and Control

The use of Private Relay raises concerns about centralisation and control - "overnight Apple will become the largest ISP in the world".

The introduction of ***Private Relay 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, who pays for interconnects and where you have to interconnect. ***By having control over so much traffic, Apple gains dominant power, or at least significant market power, in most markets, giving it the ability to dictate terms to ISPs****.*

There are far-reaching implications for the Internet, well beyond privacy, especially if the other browser and operating system vendors follow Apple's lead. The regulatory and competition aspects are of particular concern. Are there plans to legitimize Private Relay as a standard via the IETF? If so, will Google, Microsoft et al follow suit? This would lead to the end of the public Internet as it currently operates.

As noted previously, Private Relay is built on the MASQUE standards; a lot of the work on these standards within the IETF is being driven by Google at the moment.

The roundtable participants also questioned how the service will affect peering and routing? They wondered about the economic impact that Private Relay would have on the Internet ecosystem. They also questioned the level of investment that will be required to set up and operate proxy servers globally to run the service and whether there would be interest from ISPs to offer ingress proxies.

Market Dominance: A Chilling Effect on Critical Debate

Are ISPs and other organisations within the Internet ecosystem comfortable publicly criticizing Apple? ***The market dominance of Apple seems to deter companies from going on-record with concerns, something that is compounded by the partnerships that Apple has in place with organisations across the ecosystem.*** *The reluctance to criticise Apple is especially true with Private Relay: Apple has asserted that ISPs are spying on users (without offering evidence) and that Apple is therefore taking steps to stop this behaviour, hence any organisations that raises objections could be seen to be in favour of spying on users.*

One option here for ISPs that operate services and features that could be affected by Private Relay, such as zero rating of certain content, is to inform users of the implications of enabling the facility in consumer-friendly terms and let them decide whether to do so. The alternative would be to disable Private Relay at the network level by blocking the service but this results in negatively-framed dialogue being generated by Apple on user devices.

A key reason why some networks may choose not to block Private Relay is the content of the dialogue that then appears on affected Apple devices. It may also be the case that blocking access to Private Relay in some jurisdictions would place a public network operator in breach of net neutrality rules; this needs to be checked with relevant regulators.

5. Legislative and Regulatory Impacts

It is unclear whether government stakeholders have been properly briefed on the plans for the launch of Private Relay, either from Apple or from those within the ecosystem that have identified potential consequences caused by the service.

There may be issues in jurisdictions where ISPs are no longer able to meet legal or regulatory requirements because of the implementation of Private Relay, for example in the 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 in order to maintain their effectiveness. *ISPs and other stakeholders may need to ensure that national regulatory bodies and other interested parties are made aware of the potential impact of Private Relay.*

It is unclear at present whether Apple would qualify as an ISP, in Europe at least, in the strict legal sense, despite the significant share of network traffic that the company may be in a position to control. The Network Information Service Directive (NIS) applies to a range of digital infrastructure including that used for public DNS resolution, whether operated by ISPs or other entities. It is possible that, once Private Relay is enabled, Apple could be covered by this legislation as any service outage could affect network resilience. ***Regulators and others may also determine that the launch of Private Relay brings Apple into scope for other regulatory measures that are normally limited primarily to ISPs such as those relating to information retention, lawful interception etc.***

Problems may be caused where there are local sensitivities to geo-mapping of IP addresses to an alternative location. For example, in some communities people may find it unacceptable if their location is shown as being in a nearby location associated with a particular religious or ethnic group.

6. Mitigations

The impact of Private Relay on zero rated traffic is problematic, as are the implications for self-service portals as these will no longer work as expected. One option would be for Apple to implement a filter, effectively an allow list, ensuring that designated sites were not routed via Private Relay when the latter is enabled at an end point. However, this would strengthen Apple's position as gatekeeper.

Zero rating is a problem for those customers, usually less affluent, that are not on unlimited data plans (fixed or mobile), as well as for those customers on plans that include unlimited access to particular types of content (eg films, sports etc). *This may in turn lead to significant increases in inbound calls to ISP customer services when Private Relay is launched. One option could be to recommend that any customers with these packages disable Private Relay; alternatively, customers could consent to disable Private Relay when signing up to particular packages.*

Apple has stated that content on private IP addresses will fall back to using the network operator's DNS and not be routed over Private Relay. This may provide a mechanism to support zero-rated content if it is accesses via private IP addresses on host networks, especially if the same approach was taken by any others following Apple's lead with similar services to Private Relay, assuming that negative dialogue is not displayed on user devices before routing to such content.

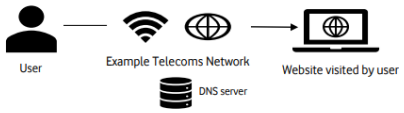
More generally, it would be helpful if users disabled Private Relay on their devices, or at least ensured that it is not enabled as a default setting. Network operators could proactively message users of affected devices to alert them to the consequences of Private Relay and provide instructions to help them change settings.

Content filtering services may well categorise services like Private Relay (and others using MASQUE etc) as anonymization or proxy services, potentially blocking access as a result. Enterprises and ISPs using content filtering should check on this as they may already be blocking Private Relay, for example for ISP customers using parental controls.

Annex

How consumers access the internet today

(simplified overview)

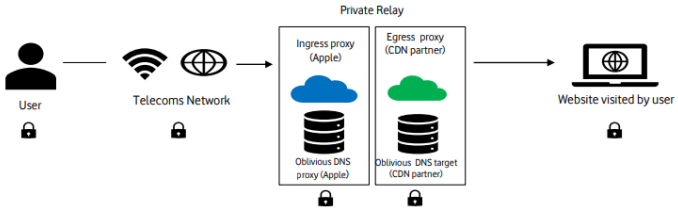


To date – an established distributed system across telecoms networks

- The Domain Name Service (DNS) is a critical but little-known part of the Internet infrastructure.
- It is used to translate a hostname (such as www.example.com) into the associated Internet Protocol (IP) addresses that allow computers to locate the right content on the Internet.
- The DNS service is provided by the telecoms network (via a distributed system, meaning each telecoms operator runs their own DNS resolver). While traditionally, a cleartext protocol was used, telecoms providers are working on deploying encrypted DNS protocols. Irrespective, the website address is still visible to the network.
- Traffic typically flows without any 3rd party proxying/tunnelling/VPNs between the user and the websites they are visiting. Some users (businesses in particular) make use of VPNs, however, they are overall a minority.
- As a result of this distributed approach and the absence of any proxying/tunnelling/VPN, telecoms networks are able to fulfil existing regulatory obligations (e.g. compliance with unlawful content blocking or security obligations)

How access to the internet works with Private Relay

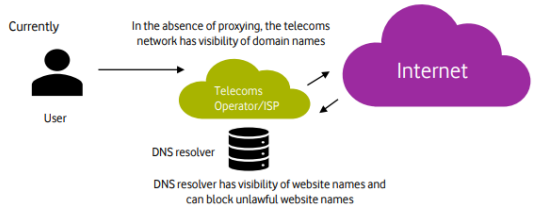
(simplified overview)



Apple's Private Relay encrypts traffic and masks the user's IP address via a new, dedicated system

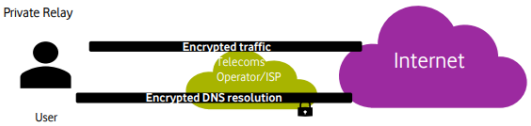
- Traffic (specifically, browser traffic for 'tracking sites' in the basic Private Relay offering, traffic for all websites in the enhanced Private Relay offering), between the user is tunnelled and encrypted by the handset, and then sent to an 'ingress' proxy managed by Apple and then forwarded to an 'egress' proxy managed by Apple's 3rd party partner.
- The proxies allocate random IP addresses to users so that websites cannot track users based on their IP address. Neither proxy knows the user's IP address and the website they are visiting. This means neither websites, nor Apple, nor the CDN partner can track users based on their IP address
- For all iCloud+ customers, the DNS server provided by the network operator is bypassed. They are replaced by DNS nodes provided by Apple and their partner which encrypts and anonymises the domain name resolution requests. This applies to not only to browser traffic DNS requests but to all the interactions (e.g. apps) between the user and the internet.
- In summary, the distributed system is replaced by a system whereby hundreds of millions of users will use a DNS resolver established by Apple.

Implications of Private Relay for blocking of unlawful content and access to public good websites



DNS blocking can be done by removing the website name entirely from all DNS servers (such as by a court order to block child pornography). Content filtering based on website name (e.g. age appropriate content) can also be performed.

Zero rating of public good websites (e.g. health or education) can be implemented by the telecoms operator in question.



As the telecoms operator's nodes have no visibility of website names, blocking is not feasible for cloud+ customers. Instead blocking would have to be done by Apple or its CDN partner.

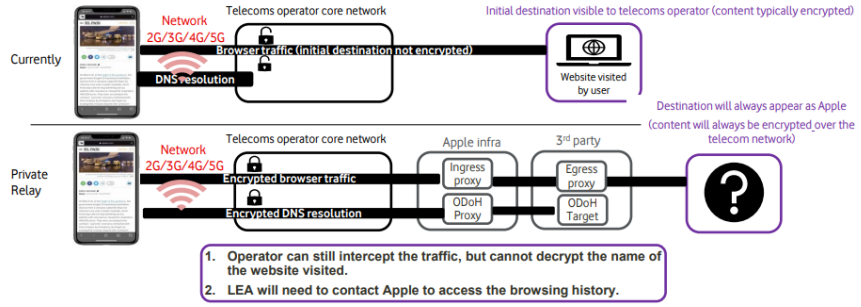
Telecoms operator is unable to block unlawful websites, perform filtering based on website name or protect against botnets.

Telecoms operator is also unable to zero rate public good websites.

Implications of Private Relay for Lawful Interception

Lawful Interception (mobile or broadband):

1. Voice calls on 2G/3G/4G & Wi-Fi– No impact on existing lawful interception capabilities
2. Safari Web browsing – interception of the names of websites visited can be performed in theory, but the operator can only identify a connection to Apple (not the actual end website). LEA will need to contact Apple.
3. This impacts both mobile and fixed line broadband services

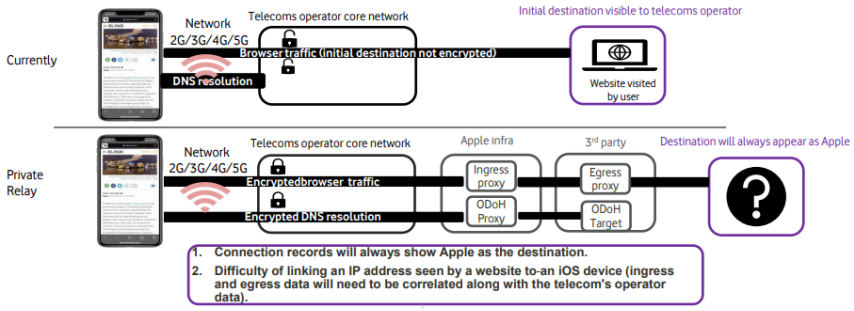


Note: The diagrams above are over simplified to focus on the impacted nodes within a telecoms network, Apple's and 3rd party infrastructure/networks

Implications of Private Relay for Data Retention and Disclosure

Retention and Disclosure of communications data

1. Voice calls on 2G/3G/4G & Wi-Fi – No impact on existing retention or disclosure capabilities
2. Safari web browsing will generate a call record, identifying a data session has occurred
3. When retained, internet connection records will only show a connection to Apple, not the actual destination.
4. Law Enforcement will not be able to resolve an IP address back to a Telecoms Operator without assistance from Apple
5. This impacts both mobile and fixed line broadband services



Note: The diagrams above are over simplified to focus on the impacted nodes within a telecoms network, Apple's and 3rd party infrastructure/networks

Implications of Private Relay for meeting Quality of Service requirements and achieving network resilience

	Current	With Private Relay
	In order to provide the most positive browsing and data experience for customers, traffic is managed and prioritised where appropriate, consistent with net neutrality regulation.	As the relevant core network traffic management nodes do not have visibility of some traffic (due to tunnelling and encryption), existing practices are in many cases not technologically feasible. This results in limited congestion management and reduced peering optimisation for data performance for traffic routed via Private Relay.
	DNS control plays a key role in relation to network performance and resilience, as it is a critical node to provide internet access to mobile customers. Operators currently have control over this capability.	Risk of Apple's proxy/DNS underperformance resulting in Private Relay users experiencing slow/lack of connectivity to certain sites/services. DNS resolution would bypass the operator .

The Quality of Service performance management methodology developed under European regulation envisages **application-specific measurement functions** such as **DNS** (manipulation of specific DNS-requests, performed by the underlying network), Audio/Video (detecting whether treatment of **audio/video** streaming might affect the performance as perceived by the end-user), Web (browsing performance) and **VoIP** (detecting how traffic to or from such applications are treated). Where there is no traffic visibility, the telecoms operator/internet access provider cannot comply with important quality of service parameters for Private Relay users.