PREISKEL & CO

MOVEMENT FOR AN OPEN WEB BRIEFING PAPER: IP ADDRESS CLOAKING

Introduction

1. Google and Apple have introduced proposals ('Gnatcatcher' and 'Private Relay', respectively). Those changes involve the "cloaking" of end users' IP addresses.

2. IP addresses exist to provide a mechanism for communication between internet locations. They are used in accordance with the internet protocol to identify the sender and the receiver of the communication. The header of each IP packet contains the IP address of the sending host and that of the destination host. Internet service providers allocate IP addresses in their network to their clients and can change them. Firewall software at homes and offices can be set up to block or control communication to and from specific IP addresses to limit spam and access to certain websites to protect users in the network. Diagnostic tools may use the IP address to identify faults and perform other tasks. Website administrators can use IP addresses to block cyberattacks and investigate fraud and illegal actions by anonymous users.

3. There are a wide variety of different uses, as described by a leading software supplier:

   "You can think of an IP address like a membership card to enter the World Wide Web. Every device that can connect to the internet is a member of the World Wide Web — computers, laptops, tablets, mobile phones, routers, etc. — and all have an IP address. Websites and computer networks require that form of identification for you to interact with them[1] … as it reveals your geolocation to help the internet deliver content that's relevant to you… For example, it's due in part to your IP address that you see local restaurants pop up when you search "sushi restaurants."

4. Authorities, including, law enforcement or fraud investigators, can also use orders to contact your ISP and get your IP address. Broadcasters and subscription services use them to block access to content available or unavailable in a specific region- in their legitimate exploitation of their intellectual property rights.

5. Many business users who compete with Google and Apple use the IP address to compete effectively in providing ads that are relevant to specific businesses or types of business by geolocation. If this information is masked, it will make it more difficult for competitors to retrieve the same information, therefore limiting their ability to do business. The competition issues have been raised with the CMA in the UK and with the EU Commission.

[1] https://us.norton.com/internetsecurity-privacy-what-does-an-ip-address-tell-you.html

IP Address in Counter-Terrorism

6. The Explanatory Notes of the Counter-Terrorism and Security Act 2015 note that IP address resolution is:

   "the ability to identify who in the real world was using an IP address at a given point in time. An IP address is automatically allocated by a network provider to a customer's internet connection, so that communications can be routed backwards and forwards to the customer."[2]

7. It is also used for various private security-based solutions, for example, for fraud prevention (to monitor when activity arises is an unusual geographic location, e.g., currency identification[3]) and spam filtering.

Google and Apple Proposals

8. Google and Apple have separately proposed (and started to implement) changes to their browsers which affect the ability of others, including ISPs, publishers' and marketers' to effectively measure performance and interactions with end users. In particular, they have proposed changes that will block the real IP address from being visible going forward. Google's proposal, 'Gnatcatcher',[4] and Apple's 'Private Relay',[5] reroute the traffic through their own anonymisation servers "cloaking" the real IP address. The data flow between the end-users browser and anonymization servers would be encrypted.

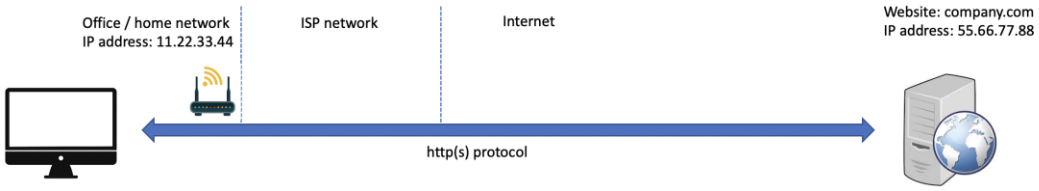

Figure 1: Diagram of the IP address without Gnatcatcher / Private Relay interference

[2] https://www.legislation.gov.uk/ukpga/2015/6/notes/division/7
[3] For example, BitGo processed digital currency transactions under its secure digital wallet management service by persons located in jurisdictions subject to a comprehensive US embargo. This was due to a deficiency in BitGo's sanctions compliance procedures. However, BitGo was able to identify the persons involved in sanctioned jurisdictions based on IP address data associated with their devices and account login location. See: https://home.treasury.gov/system/files/126/20201230_bitgo.pdf
[4] https://developer.chrome.com/en/docs/privacy-sandbox/gnatcatcher/
[5] https://developer.apple.com/support/prepare-your-network-for-icloud-private-relay/

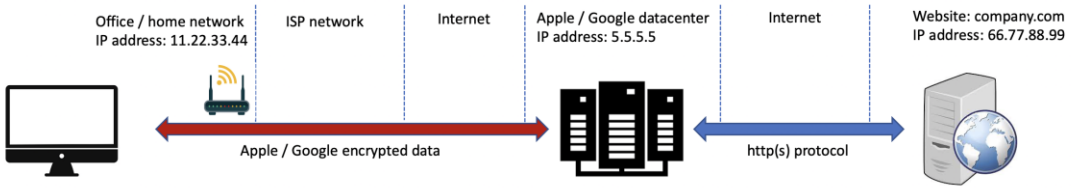

Figure 2: Diagram of the IP address after implementation of Gnatcatcher / Private Relay

9. Some ISPs (Vodafone, Telefonica and T-Mobile) have requested the EU Commission ban the implementation of both proposals, given it cuts off networks and servers from accessing "vital network data and metadata", resulting in "significant consequences in terms of undermining European digital sovereignty" and also impacts "operator's ability to efficiently manage telecommunication networks".[6]

Duties under national security legislation

10. The Regulation of Investigatory Powers Act 2000, Data Retention and Investigatory Powers Act 2014, and Counter-Terrorism and Security Act 2015 all impose duties on communication services providers to retain a category of data and information that links the unique attributes of a public IP address to a person or device using it at any given time. These obligations are imposed in the interests of, *inter alia*, national security and preventing or detecting crime.

11. If Gnatcatcher and Private Relay are to encrypt all data passing through ISP network from end-user to the anonymization servers and clock the real IP address, this could preclude ISPs from fulfilling their duties. This may impede efficient enforcement of national security policy and legislation.

12. Given ISPs will be unable to obtain the data they may have a legitimate excuse for non-compliance with law enforcement requests. The Investigatory Powers Act 2016 allows for ISPs, *inter alia*, to retain information and data for the purposes of law enforcement (i.e., interception warrant on the grounds of national security, economic wellbeing in the UK or in support of the prevention or detection of serious crime). If they have no such data, they cannot easily be compelled to deliver it to law enforcement.

Effects of Google and Apple Proposals on different parties

13. Gnatcatcher and Private Relay have a debilitating effect on the following:

    a. ISPs

[6] https://9to5mac.com/2022/01/10/european-carriers-seek-to-block-iphone-private-relay-feature/

i. ISPs will only see encrypted data flowing from users to Apple and Googles' ecosystems.
ii. ISPs will find it harder to monitor real traffic because of the cloaking proposals.
iii. ISPs will no longer be able to offer content filtering services or other security services to people at homes and offices.
iv. Duties imposed by the Investigatory Powers Act will be made more difficult or impossible to fulfil.[7]

b. Office / home networks
   i. Routers only see encrypted data going to Apple and Google
   ii. Parents are unable to protect children from inappropriate or malicious websites via content filtering services if they are unable to monitor information being passed along the IP address.[8]
   iii. Companies, both at a managerial level and employee level, will suffer for similar reasons if content filtering is prevented. Companies become more susceptible to spam and are unable to restrict websites on their own networks.

c. Websites, publishers, advertisers, service providers
   i. Difficult to prevent and investigate fraud and hacking. Protection will be reduced, and investigation timeframes will be increased significantly. [9]
   ii. Impossible to control access using IP addresses.
   iii. Impossible to carry out IP-based B2B website personalisation, analytics and advertising. B2B advertising revenues are driven to Google and Apple instead.

d. End users
   i. Network response times will be slower, leading to a decrease in consumer/user experience.

e. Law enforcement agencies
   i. The inaccessibility of data and information passed along the IP address makes it more difficult, if not impossible, to investigate criminal activity online.
   ii. If information is requested from Google or Apple, they may be able to respond that they do not have it and this may delay the investigation

[8] https://hitechglitz.com/apples-private-relay-service-poses-challenges-for-uk-isps/
[9] Part II of the 2000 Act provides for notices requiring disclosure of data protected by encryption. It is an offence not to comply with such a notice. However, this is a procedural hurdle that enforcement authorities will have to go through every time they require information from Google and Apple's systems to prevent and combat national security concerns.

process and compromise the time-sensitive nature of law enforcement, detection and prevention.

f. Google and Apple are giving themselves a greater ability to control all data flow between browsers and websites and to offer services that have been rendered impossible for others to provide in competition. Whilst this may favour Google and Apple, it is also of significant concern.

Next Steps

14. Google and Apple claim to implement these proposals in the name of improving and safeguarding user privacy.

15. If there is a real risk to privacy arising from IP addresses being used in conjunction with other data to identify individuals illegitimately, protecting consumer privacy would more easily be achieved by ISPs rotating or reallocating IP addresses on consumer connections. This would render Private Relay and Gnatcatcher unnecessary and would effectively address the concerns that Google and Apple have raised, but without damaging competition or compromising law enforcement.