BT Group response to Mozilla Trusted Recursive Resolver Consultation

Respecting privacy and security

1. Our current policy states that user data must not be retained for longer than 24 hours. A number of DNS providers, however, only keep data in ephemeral state and delete it almost immediately.
   a. To what extent can our requirement be shortened further while allowing providers sufficient data to operate the service?

BT response: From a UK/European perspective length of data retention should be as per local in country data protection and privacy legislation. It should be noted that there may be regulatory and operational service requirements that may require data retention in excess of 24 hours, e.g. for troubleshooting customer and service issues.

   b. What operational constraints, if any, are created by this maximum 24-hour retention time?

BT response: This may conflict with in-country regulatory requirements and service operations, e.g. ability to troubleshoot customer and wider service issues.

2. Are there exemptions that should be allowed by the policy for additional data collection in emergency circumstances? Please specify (e.g., the relevant circumstances as well as transparency and reporting requirements).
   No response

3. Our existing agreements stipulate that providers in our TRR program shall undergo third-party audits to confirm compliance with our TRR policies; are there particular criteria (e.g., auditor qualifications) or considerations (e.g., cost) that we should take under advisement?

BT response: Costs of third-party audits are an important consideration and requiring extensive auditing could risk excluding smaller providers, including specialised UK ISPs, from becoming a TRR partner. There is also a question to what degree third-party auditing would deliver any meaningful benefits to users whose current providers already operated within the heavily regulated UK telecommunications and data protection framework. As a result, there is a clear risk that third-party auditing requirements will lead to a further centralisation of DNS-resolution. However, clearly transparency and compliance are important, so a lightweight and low-cost audit option, if one could be designed, would mitigate this concern."

4. Our current policy establishes that DoH resolvers in our program must maintain a transparency report providing public insight into the extent to which the resolver has been subject to government requests for data. How can this requirement be improved? What other mechanisms, processes, and governance tools may exist that could provide the public additional insight into such requests?

BT response: Resolver operators will be unable to meet any transparency requirements which contradict legal secrecy requirements around the use of investigatory powers in their jurisdictions of operation.

In the past year, emerging legislation such as the UK Online Harms framework or the EU Digital Services Act have also introduced the possibility of statutory transparency reporting obligations in relation to online harms. Ensuring that any transparency requirements associated with the TRR programme are in-line with these developments would facilitate their uptake by providers. The TRR could also draw on comparable transparency guidance from the Global Network Initiative (GNI) or the Sustainability Accounting Standards Board (SASB).

Online Safety

1. Our current policy states that the provider operating the resolver should not by default block or filter domains unless specifically required by law in the jurisdiction in which the resolver operates. How, if at all, should this requirement change to address legally required blocking in other jurisdictions?
BT response: Providers operating the resolver will need to comply with the blocking legal requirements of the jurisdictions that they operate in.

2. What harmful outcomes can arise from filtering/blocking through the DNS?
BT response: Harmful outcomes may result from over-blocking or under-blocking (missing websites that should be blocked). Both risks are mitigated by having opt-in models and options for customers to configure the level of protection they see as appropriate to them, and also clear and easily accessible processes for customers to contact the filtering/blocking provider.

3. What more rights-protective and technically effective means of protecting users from illegal and harmful content exist beyond DNS-based blocking?
BT response: Endpoint parental controls and endpoint anti-virus are other effective means of protecting users from illegal and harmful content that do not require DNS-based blocking. However, they have poor adoption due to requiring installation on devices, lack interoperate-ability across platforms, and typically are chargeable. This makes these alternatives challenging to achieve mass adoption. Furthermore, alternative deep packet inspection network filtering will be impacted by the future adoption of ESNI/ECH.

4. How could we ensure effective transparency and accountability in situations where TRRs engage in legally required blocking practices? (For example: publicly available transparency reports with blocked domain names by country.)

BT Group response to Mozilla Trusted Recursive Resolver Consultation

BT response: TRRs could explain on their website or in a publicly available transparency report the circumstances when they are legally required to block including a list of court-order based blocked sites. Court orders are publicly held information and are matters pertaining to public safety.

a. What governance, process, or audit requirements should be required of parties that maintain and create block lists? For example, what complaint and redress processes should exist?

BT response: As a standard, there should be a clear and easily accessible process for customers to query providers specifically about website blocking or categorisation and this should be handled by a dedicated team who respond to customers query within a defined SLA, preferably no later than 1-2 days for an actual re-categorisation (if found to be wrong). In the UK, for mobile there is independent arbitration by the BBFC which customers can contact directly – more information can be found at https://www.bbfc.co.uk/about-classification/mobile-content/framework

b. What challenges weigh against a requirement to publish block lists?

BT response: Only court order based blocking should be published, otherwise cyber criminals will know what is being blocked and will be able to game domains. There is no independent arbitration for broadband parental controls website categorisation as there is for mobile (through the BBFC), so each ISP has potentially slightly different view on website categories – and by exposing all of the categorisation there is a risk of having to provide complex and time consuming explanations to customers.

5. How can we best present information about opt-in filtering endpoints to end users (e.g., for malware blocking or family-friendly blocking)?

BT response: Dashboards could inform customers about what domains have been blocked and why, including which devices in the home have blocking.

<u>Building a better ecosystem</u>

1. How can deployment of DoH help to increase trust in Internet technologies in your region?

BT response: BT always looks favourably upon emerging technologies that improve security and privacy for our customers, however in the cases of DoH, ESNI/ECH and MAC randomisation further standardisation work is required across the end to end ecosystem to address unintended consequences to ISP customer experience, on-line safety and in country regulatory obligations.

2. What exploitations of the DNS in your region could DoH protect against?

No response

BT Group response to Mozilla Trusted Recursive Resolver Consultation

3. What are the best ways to gain global adoption/support of the DoH standard amongst ISPs and DNS providers?

BT response: A key blocker for European ISPs is the availability of a DNS over HTTPS discovery standard that will work with existing home hubs / customer premise equipment that use DNS over port 53 proxies that only present private IP addresses to clients.

4. Are there specific DNS use cases for which you think DoH would provide particular security and privacy value (e.g., when users connect over free public WiFi hotspots)?

BT response: ISPs may wish to offer a DoH service to their customers when away from their normal network. This could enhance security and enable continuity of service features when using free public WiFi. The use of such non-local DoH should require initial consent from the user but could then be automatic.

5. Although Firefox disables DoH when it detects that enterprise policies are in place, are there other situations in which deployment of DoH might cause technical or operational challenges (e.g., mobile networks, NAT64 and DNS64)?

BT responses: Changing the provider of DNS resolution can cause many challenges, such as DNS64 as you note. Enterprises expect to be involved in the DNS resolution process in order to provide some security against attack. However, the need for such security is not unique to enterprises. Home users also need security, and the need for this will grow over time as IoT devices proliferate. Hence the challenge is to ensure that upgrade to DoH does not involve a change of provider, or if it does, that the new provider does not involve a weakening of any aspect of security.