419.Consulting

New European Policy Sets Standards for Privacy and Transparency

London, Wednesday 30th March 2021

A new initiative, formulated by experts from across the technology and telecoms sectors, has been launched to protect personal data. The new "European DNS Resolver Policy" has been designed to ensure that companies have clear privacy and transparency policies that are easily accessible, setting out how any personal data is used and whether it is exploited commercially.

A critical but little-known part of the Internet infrastructure outside of the technical community is the Domain Name Service (DNS). This is the mechanism used to translate website names into the associated Internet Protocol (IP) addresses that allow computers to locate the right content on the internet. It is the Internet's equivalent of a directory service to translate between the memorable names that are useful to humans and the Internet addresses needed by computers.

The translation between website names and IP addresses is referred to as "resolution", and the companies that run the services are called resolver operators. Often the resolver operators are ISPs but there are many other companies that provide standalone services, including some run by large technology companies.

When examining the current policies used by resolver operators, some do not recognise key legislation such as GDPR and ePrivacy, being more suited to the US market where their authors reside. In addition, not all policies cover key elements such as the jurisdiction under which they operate, with the resulting ambiguity being unhelpful to users.

Many of the tasks on our computers make use of the DNS, potentially allowing the companies that operate the system to track the activities of users without their knowledge. The new "European DNS Resolver Policy" lays out clear standards for the operators of such systems, setting expectations regarding the collection, use and retention of personal data. It also outlines how companies can state whether they protect users from malicious content and provide parents with tools to manage the activities of their children.

> The policy's author, Andrew Campling, director of 419 Consulting, said: "We've worked with a wide range of organisations across Europe and North America to develop this new policy document. It sets out clear expectations of behaviour for companies as well as specifying what information should be made available to users"
>
> He added: "The European Resolver Policy encourages the operators of a critical part of the Internet infrastructure to commit to higher levels of privacy and security. The adoption of the resolver policy by operators will give reassurance to users that their privacy is protected and their personal data is not being monetised without their knowledge."

A key distinction of the new policy is that it makes direct reference to the European Union's General Data Protection Regulation (GDPR) as well as to national legislation. The policy is designed to apply to both standard and encrypted DNS, including the recently introduced DNS-over-HTTPS ("DoH") protocol.

More information about the European DNS Resolver Policy can be found at https://EuropeanResolverPolicy.Com. Companies can sign up to use the European DNS Resolver Policy at no cost by contacting Enquiry@EuropeanResolverPolicy.Com.

ENDS

FAQs

1. Where can I find more details about the content of the European DNS Resolver Policy?

   Full details are available on the website which can be accessed at https://www.EuropeanResolverPolicy.Com. Please contact the team at Enquiry@EuropeanResolverPolicy.Com if you have any questions.

2. What are the main benefits that the new policy brings to Internet users?

   Companies that sign up to the policy must have transparency and privacy policies that give clear, easily accessible information about the way that any personal data of users is stored and used. They commit to make technology and operational choices that protect user privacy.

3. Don't existing regulations give users sufficient protection?

   Some of the companies that operate DNS services are based offshore and so enforcement of local regulations can be difficult. Companies that commit to the European DNS Resolver Policy agree that their services will be operated in a manner that matches or exceeds the protections described in all relevant EU Directives and Regulations as well as by the national regulations of the jurisdiction(s) in which they are based.

4. How can I find details of companies that have adopted the policy?

   As companies adopt the European DNS Resolver Policy, their details will be added to the policy's website and they can of course reference their compliance in their own literature.

5. What happens if an organisation is found to be non-compliant?

   If a company that has previously adopted the resolver policy is subsequently found to be non-compliant then it will be given an opportunity to address the shortcomings. If action is not taken promptly then the company will be removed from the list of compliant organisations with a note added to indicate the reason for the removal.

6. Who is behind the new policy?

   Although the policy has been written by 419 Consulting, a public policy consultancy, experts from many organisations drawn from across the industry, mainly based in Europe and North America, have helped develop and agree the content. These organisations include Internet Service Providers, software companies, technology companies and policy advisors. Input has also been provided by civil society groups, regulators and other key stakeholders.

7. Does the new policy cover all types of DNS including the most recent encrypted DNS standards?

   Yes, the policy is designed to be independent of the type of DNS so covers systems using the original DNS standard as well as more recent, encrypted standards including DNS-over-TLS (DoT) and DNS-over-HTTPS (DoH) and emerging protocols such as DNS-over-QUIC (DoQ),.

8. What types of organisations are expected to adopt the new policy?

   It is targeted at a range of companies including Internet Service Providers (ISPs) and specialist technology companies that operate DNS services. Other organisations including software developers, industry regulators and legislators may wish to endorse the policy and encourage its adoption.

9. How can my organisation adopt the policy?

   The policy is accessible at https://www.EuropeanResolverPolicy.Com. Once your processes have been adapted and your transparency and privacy reports updated to reflect the changes, you can contact the team at Enquiry@EuropeanResolverPolicy.Com to confirm that you are committing to remain compliant.

10. Are there any charges for companies to adopt the European DNS Resolver Policy?

    No, it is an industry initiative that any organisation is free to join.