ICANN Perspectives on EU Digital Initiatives

A Stakeholder Assembly Presenting ICANN org Reflections on Current European Union Initiatives

15:00 UTC
27 January 2021
Chris Mondini
Vice President of Stakeholder Engagement in Europe & Managing Director, Brussels
chris.mondini@icann.org
Welcome – Chris Mondini

EU initiatives relevant to the DNS – Elena Plexida
- The Digital Services Act (DSA)
- The Digital Market Act (DMA)
- EU Cybersecurity Strategy for the Digital Decade

Potential Technical and Operational Impacts – David Conrad

Considerations for ICANN community and policy making – Elena Plexida

Q&A – Chris Mondini

Conclusion - Chris Mondini
EU initiatives relevant to the DNS

Elena Plexida
Vice President
Government and IGO Engagement

elena.plexida@icann.org
EU Initiatives Relevant to the DNS

In December 2020, the European Commission published important initiatives relevant to the DNS including domain name registration data and DNS services providers:

- The Digital Services Act package, comprising of:
  - the Digital Services Act (DSA) and
  - the Digital Markets Act (DMA)

- The new EU Cybersecurity package that includes:
  - A "Communication on the EU’s Cybersecurity Strategy for the Digital Decade"
  - A Directive on the resilience of critical entities
The Digital Services Act (DSA)

The Digital Services Act (DSA) introduces new EU-wide obligations on illegal content which will apply to digital services that offer to consumers goods or services.

The new law is a reform of the 2000 e-Commerce Directive.

It broadens the scope of the e-Commerce Directive and enhances obligations for companies that own a great size of the market and have a great impact on European users.

The DSA also introduces rules on transparency of content moderation algorithms.

Noteworthy regulatory aspects:

- Exterritoriality effect
- Does not specify “illegal content”
- Preserves some key features of the e-Commerce Directive

New oversight structure, Member States will have the primary oversight role, supported by a new coordination body, the European Board for Digital Services.
The Digital Services Act (DSA)

Scope

- **Intermediary services** offering network infrastructure: Internet access providers, domain name registrars, including also:
- **Hosting services** such as cloud and webhosting services, including also:
- **Online platforms** bringing together sellers and consumers such as online marketplaces, app stores, collaborative economy platforms and social media platforms.
- **Very large online platforms** pose particular risks in the dissemination of illegal content and societal harms. Specific rules are foreseen for platforms reaching more than 10% of 450 million consumers in Europe.
Exemption of Liability

Provisions on the exemption of liability of providers of intermediary services

- DSA includes conditions under which providers of mere conduit (Article 3), caching (Article 4) and hosting services (Article 5) are exempt from liability for the third-party information they transmit and store;

- The liability exemptions should not be disapplied when providers of intermediary services carry out voluntary own-initiative investigations or comply with the law (Article 6);

- Prohibition of general monitoring or active fact-finding obligations for those providers (Article 7);

- Obligation on providers of intermediary services in respect of orders from national judicial or administrative authorities to act against illegal content (Article 8) and to provide information (Article 9).
Obligations applicable to providers of intermediary services

- Obligation to establish a single point of contact to facilitate direct communication with Member States’ authorities, the Commission and the Board (Article 10);

- Obligation to designate a legal representative in the Union for providers not established in any Member State, but offering their services in the Union (Article 11);

- Obligation to set out in their terms and conditions any restrictions that they may impose on the use of their services and to act responsibly in applying and enforcing those restrictions (Article 12);

- And transparency reporting obligations in relation to the removal and the disabling of information considered to be illegal content or contrary to the providers’ terms and conditions (Article 13).
Obligations on Hosting Services

Obligations applicable to providers of hosting services

- Put in place mechanisms to allow third parties to notify the presence of alleged illegal content (Article 14);

- Furthermore, if such a provider decides to remove or disable access to specific information provided by a recipient of the service, the provider is obliged to provide that recipient with a statement of reasons (Article 15).
The Digital Market Act (DMA)

Scope

- Companies subject to the DMA are “core platform services”, meaning companies that own a considerable portion of EU’s market.

Key provisions

- The DMA aims at preventing gatekeepers from imposing unfair conditions on businesses and consumers.

- It forbids conducts such as prohibiting businesses from accessing their own data when operating on these platforms; and / or compels gatekeepers to proactively implement certain practices, such as allowing business users to access their own data.

- Infringements can lead to a fine of 10% of the company's total worldwide annual turnover and periodic penalty payments of up to 5% of the company's total worldwide annual turnover.
The Communication on the EU's Cybersecurity Strategy for the Digital Decade outlines a variety of initiatives the Commission will undertake in the course of the 2019-2024 mandate in the field of cybersecurity, such as:

- Establish a Joint Cyber Unit, in charge of coordinating cybersecurity operations between the Commission, Member States and other relevant bodies (ENISA or Europol). In this context, the Commission will search input from industry and partners in the process.

- Seek to implement its agenda against cybercrime; enhance the overall EU’s capabilities in deterring malicious cyber activities.

- Consider introduction of qualified majority voting in the Council for sanctions against cyber-attacks and seek further cooperation with NATO.
Section 1.6 titled "Greater global Internet security" puts forward a number of actions related to the DNS:

- develop a contingency plan, supported by EU funding, for dealing with extreme scenarios affecting the integrity and availability of the global DNS root system
- encourage EU companies, ISPs and browser vendors to adopt a DNS resolution diversification strategy
- contribute to secure Internet connectivity by supporting the development of a public European DNS resolver service - the 'DNS4EU' initiative
- in liaison with Member States and industry, accelerate the uptake of key internet standards including IPv6 and well-established internet security standards and good practices for DNS, routing, and email security
- consider the need for a mechanism for more systematic monitoring and gathering of aggregated data on Internet traffic and for advising on potential disruptions
The NIS2 Directive

- NIS2 applies to all providers of DNS services along the DNS resolution chain, including operators of root name servers, TLD name servers, authoritative name servers for domain names and recursive resolvers.
- It includes a definition of the DNS
- It includes a definition of DNS service providers
- No identification system by the EU Member States
- A DNS service provider must designate a representative under NIS2, in cases in which a DNS service provider not established in the EU offers services within the EU.
- Single jurisdiction regime
- NIS2 Directive recognizes that “Maintaining accurate and complete databases of domain names and registration data (so called ‘WHOIS data’) and providing lawful access to such data is essential to ensure the security, stability and resilience of the DNS.”
The NIS2 Directive

Article 23 “Databases of domain names and registration data” of NIS2 would require EU Member States to ensure that domain name registries and registrars take several actions related to registration data:

- collect and maintain accurate and complete domain name registration data in a dedicated database facility with due diligence subject to Union data protection law as regards data which are personal data.

- ensure that the databases of domain name registration data contain relevant information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs.

- have policies and procedures in place to ensure that the databases include accurate and complete information and that such policies and procedures are made publicly available.

- publish, without undue delay after the registration of a domain name, domain registration data which are not personal data.

- provide access to specific domain name registration data upon lawful and duly justified requests of legitimate access seekers, in compliance with Union data protection law; reply without undue delay to all requests for access; make policies and procedures to disclose such data publicly available.
Potential Technical and Operational Impacts

David Conrad
Chief Technology Officer
david.conrad@icann.org
Realization that digital services have profoundly changed the way EU citizens live and do business.

- Array of existing national jurisdictions is seen as insufficient.

Lots of operational/technical considerations for the ICANN community:

- For multi-national “intermediary service providers”, operations should be simplified
  - Don’t have to deal as much with varying national regulatory requirements
- For all but “small and micro” service providers
  - Fairly detailed set of obligations for various services and handling “illegal content”
  - For “very large” service providers, formal risk assessment of systemic risks, with reasonable efforts towards mitigations
- For states, a new role “Digital Service Coordinator”
- Impact for ICANN community members unclear
  - DNS explicitly called out, albeit for “conduit of information”, not source of information
    - Resolver operators and third-party authoritative providers probably exempt
    - Clarification probably needed for registries and registrars
EU Cybersecurity Strategy

- Observes critical/core protocols and components on the Internet are increasingly centralized and centralized outside of the EU
- Encourages EU organizations to adopt a “DNS diversification strategy”
  - Supports a European public DNS resolution service “DNS4EU”
- Commission to work with/fund several European parties, including 2 European root operators (Netnod and RIPE-NCC) "to deal with extreme scenarios affecting the integrity and availability of the global DNS root system."
  - Includes “re-assessing the role of the two EU root server operators in guaranteeing that the Internet remains globally accessible, no matter the circumstances.”
- Commission to support the deployment of IPv6, DoH, DMARC/DKIM, and routing security best practices
- Not intended to create a “European Internet”, rather to deal with extreme scenarios
  - The Commission will be more active in the deployment of DNS security standards
  - Will work with ICANN and the multi-stakeholder community
Directive on Security of Network and Information Systems (NIS2)

- A proposal for a revision of the 2016 NIS, bringing greater capabilities, cooperation and cybersecurity risk management.
  - Stricter supervision through reporting obligations and enforcement of sanctions
  - Additional sectors covered
  - Establishes EU Cyber Crises Liaison Organization Network (EU-CyCLONe)
  - Improves cybersecurity risk management

- ICANN community related impact
  - ENISA to maintain a registry of member state jurisdiction of essential services (Non-EU need a representative)
  - Authorities to supervise compliance with security and notification requirements with fines for violations
  - Applies to all providers of DNS services along the DNS resolution chain
  - TLD registries and the entities providing domain name registration services for them (TLD entities) shall:
    - Collect and maintain accurate and complete domain name registration data.
    - Provide efficient access to domain registration data for legitimate access seekers.
    - Establish policies and procedures to collect and maintain accurate and complete registration data.
    - Prevent and correct inaccurate registration data in accordance with Union data protection rules.
    - Respond without undue delay to requests from legitimate access seekers for the disclosure of domain name registration data.
    - Establish policies and procedures for the publication and disclosure of registration data, including service level agreements to deal with requests for access from legitimate access seekers.
Considerations for ICANN Community and Policy Making

Elena Plexida
Vice President Government and IGO Engagement
elena.plexida@icann.org
Chris Mondini
Vice President of Stakeholder Engagement in Europe & Managing Director, Brussels
chris.mondini@icann.org
Contact information and publications

Chris Mondini
chris.mondini@icann.org

Elena Plexida
elena.plexida@icann.org

David Conrad
david.conrad@icann.org

ICANN Government Engagement and OCTO publications

ICANN Government Engagement
https://www.icann.org/resources/pages/government-engagement-publications-2020-03-02-en

ICANN OCTO publications
Nordic Region Workshop: ICANN and its Technical Mission

• 3 March 2021

• To strengthen knowledge and raise awareness on matters concerning ICANN’s role in the technical functions of the internet and inform about ICANN’s key technical projects;

• For anyone interested in the technical functions of the internet;

• Aiming at Nordic Region, but everyone is welcome!

• Agenda & Registration: https://features.icann.org/event/icann-organization/nordic-region-workshop-icann-and-its-technical-mission

• Questions: Gabriella Schittek gabriella.schittek@icann.org
Sign up for our newsletter

Go to www.icann.org and click on NEWS & MEDIA. Then choose Global Newsletters from the dropdown.