Impact of Regulatory Developments on ICANN Policy Topics

Monday, 14 June 2021
12:30-14:00 CEST
Program

Part 1
Overviews

Part 2
Panel Discussion

Part 3
Community Discussion
**Participants**

Joanna Kulesza  
Moderator

**Part 1**

- Olivier Bringer  
European Commission
- Alexander Seger  
Council of Europe

**Part 2**

- Fred Baker  
Root Server System Advisory Committee Chair
- Philippe Fouquart  
Generic Names Supporting Organization Council Chair
- Matthias Hudobnik  
At-Large Advisory Committee Member
- Alejandra Reynoso  
Country Code Names Supporting Organization Council Chair
Part 1

Overviews
1. Proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS2)

2. Proposal for a Regulation on a Single Market For Digital Services (Digital Services Act)
Three main pillars of the proposal for NIS 2

**MEMBER STATE CAPABILITIES**
- National authorities
- National strategies
- CVD frameworks
- Crisis management frameworks

**RISK MANAGEMENT**
- Accountability for top management for non-compliance
- Essential and important companies are required to take security measures
- Companies are required to notify incidents

**COOPERATION AND INFO EXCHANGE**
- Cooperation Group
- CSIRTs network
- CyCLONe
- CVD and European vulnerability registry
- Peer-reviews
- Biennial ENISA cybersecurity report
NIS2 and the DNS

**Critical role of the DNS** recognised: a reliable, resilient and secure DNS is a key factor in maintaining the integrity of the Internet

**Scope** - all providers of DNS services along the DNS resolution chain, including operators of root name servers, top-level-domain (TLD) name servers, authoritative name servers for domain names and recursive resolvers.

DNS service providers and TLDs are **automatically in scope**, no identification from Member States.

**Single jurisdiction regime**: main establishment; **non-EU entities** to designate a representative in the Union

**Security measures horizontally** identified in NIS2 but **sector-specific** implementing acts will be possible

**Responsibility** anchored at the level of the management bodies of the essential and important entities
NIS2 and domain name registration data

**Importance of domain name registration data:** “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, which in turn contributes to a high common level of cybersecurity within the Union.”

**Availability and accessibility of the data:** “The availability and timely accessibility of these data [...] is essential to prevent and combat Domain Name System abuse, in particular to prevent, detect and respond to cybersecurity incidents.”
NIS2 and domain name registration data: Article 23

- Obligations concern TLD registries and entity providing registration services for the TLD
  - Collect and maintain accurate and complete domain name registration data.
  - Contain relevant information to identify/contact holders and contact points.
  - Publish non-personal data without undue delay.
  - Ensure all requests to access domain name registration data receive a reply without undue delay.
  - Provide access to specific personal data upon duly justified requests by legitimate access seekers
- EC can adopt guidelines
The Digital Services Act in a nutshell

Ambitious reform for the EU to re-structure its own informational space & set global standards

Modernise the rules to more effectively address illegal content and systemic risks in the online space

Ground rules for a truly competitive Single Market for digital services, with legal clarity and effective supervision of digital services

Clarify the rules on liability, giving companies legal certainty to take voluntary action in a diligent and proportionate manner under clear terms of service

Ensuring trust across EU MS, supporting cross-border cooperation among national authorities

Increase transparency, accountability, facilitate better oversight
Intermediary services

- offering network infrastructure: Internet access providers, domain name registries, wifi hotspots...

Hosting services

- such as cloud infrastructure & webhosting services

Online platforms

- E.g. online marketplaces, app stores, or collaborative economy platforms or social media platforms

Very large online platforms

- Specific rules for platforms reaching 45 million users (10% EU population)
### DSA - Due diligence obligations

<table>
<thead>
<tr>
<th>OBLIGATIONS</th>
<th>VERY LARGE PLATFORMS</th>
<th>ONLINE PLATFORMS</th>
<th>HOSTING SERVICES</th>
<th>ALL INTERMEDIARIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Points of contact</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Legal representatives</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Terms and conditions</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Transparency reporting</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Notice &amp; Action</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Statement of reasons</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Complaint handling</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Out of Court Dispute Settlement</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Trusted flaggers</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Abusive behaviour</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Know Your Business Customer (KYBC)</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Reporting criminal offences</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Advertising transparency</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Additional transparency reporting</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Risk assessment and mitigation</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Independent audits</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Recommender systems</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Enhanced advertising transparency</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Data access and scrutiny</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Compliance officer</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Enhanced Transparency reporting</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>

**Cumulative obligations**
What does the DSA bring for the DNS?

- **Certainty** of being covered by the **EU legal framework** (recital 27)

- **Proportionality** when tackling illegal content online: number of mitigation measures + subsidiarity (recital 26)

- **Harmonised framework**: clarification how the Member State can request to act against illegal content (art. 8)

- Overall **balanced solution** as far as infrastructural services providers are concerned

2nd Additional Protocol to the Budapest Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence: Update

Alexander Seger
Head of Cybercrime Division
Council of Europe
www.coe.int/cybercrime
Budapest Convention: a global framework for cooperation on cybercrime

Budapest Convention on Cybercrime:

1. Specific offences against and by means of computer systems
2. Procedural powers with safeguards to investigate cybercrime and collect electronic evidence in relation to any crime
3. International cooperation on cybercrime and e-evidence

+ Guidance Notes

+ Protocol on enhanced cooperation on cybercrime and electronic evidence in preparation

By June 2021: 66 Parties and 11 Observer States

“Protecting you and your rights in cyberspace”

Cybercrime Convention Committee (T-CY)

Cybercrime Programme Office (C-PROC) for capacity building
Why a new Protocol?

- The scale and quantity of cybercrime, devices, users and victims
- Cloud computing, territoriality and jurisdiction
  - Where is the crime?
  - Where is the data, where is the evidence?
  - Who has the evidence?
  - What legal regime applies to order / disclose data?
- The challenge of mutual legal assistance
- The “<1% problem”

- How to obtain subscriber information more efficiently?
- How to cooperate directly with a service provider in another Party?
- How to obtain WHOIS data (domain name registration information) from registrars? What legal basis?
- How to obtain stored data, including content, in an emergency situation?
- How to make mutual assistance more effective?
- How to reconcile efficient and effective measures with rule of law and data protection requirements?
2nd Additional Protocol: the process

- Preparatory work of the Cybercrime Convention Committee (T-CY):
  - Transborder Group (2012-2014)
  - Assessment of MLA provisions (2014)
  - Need for Protocol identified

- T-CY 17 (June 2017): Terms of reference adopted

- 10 Drafting Plenaries + 16 Drafting Group meeting + 65 virtual subgroup meetings + 6 rounds of consultations + numerous bi/trilateral meetings + domestic meetings

- Approved by the T-CY on 28 May 2021

- Formal adoption expected November 2021 & opening for signature Spring 2022
## Content of the (draft) Protocol

### Preamble

### Chapter I: Common provisions
- Article 1 Purpose
- Article 2 Scope of application
- Article 3 Definitions
- Article 4 Language

### Chapter II: Measures for enhanced cooperation
- Article 5 General principles applicable to Chapter II
- **Article 6 Request for domain name registration information**
- Article 7 Disclosure of subscriber information
- Article 8 Giving effect to orders from another party for expedited production of subscriber information and traffic data
- Article 9 Expedited disclosure of stored computer data in an emergency
- Article 10 Emergency mutual assistance
- Article 11 Video conferencing
- Article 12 Joint investigation teams and joint investigations

### Chapter III – Conditions and safeguards
- Article 13 Conditions and safeguards
- **Article 14 Protection of personal data**

### Chapter IV: Final provisions
- Article 15 Effects of this Protocol
- Article 16 Signature and entry into force
- Article 17 Federal clause
- Article 18 Territorial application
- Article 19 Reservations and declarations
- Article 20 Status and withdrawal of reservations
- Article 21 Amendments
- Article 22 Settlement of disputes
- Article 23 Consultations of the Parties and assessment of implementation
- Article 24 Denunciation
- Article 25 Notification
Article 6 – Request for domain name registration information

6.1 Each Party shall empower its authorities to issue a request to a “registrar”* for information to identify or contact the registrant of a domain name … subject to reasonable conditions provided by domestic law

6.2 Each Party shall permit a “registrar” in its territory to disclose information in response to a request issued by another Party

6.3 The request shall include:
   • Identity/contact information of authority issuing the request
   • The domain name about which information is sought
   • What information is sought
   • name, address, telephone, email
   • Fact that request is issued pursuant to the Protocol
   • Fact that request is related to specific criminal investigation
   • Only to be used for that investigation
   • How/when to disclose the information

6.5 Consultation in case of non-cooperation

* An “entity providing domain name registration services”

ER paragraph 76:
- The objective of Article 6 is to provide an effective and efficient framework to obtain information for identifying or contacting the registrant of a domain name.
- The form of implementation depends on the Parties’ respective legal and policy considerations.
- This article is intended to complement current and future internet governance policies and practices.
Article 6 – Request for domain name registration information

ER 83:
This article does not require Parties to enact legislation obligating these entities to respond to a request from an authority of another Party. Thus, the entity offering domain name registration services may need to determine whether to disclose the information sought. This Protocol assists with this determination by providing safeguards that should facilitate the ability of entities to respond to requests under this article without difficulty, such as:

— this Protocol provides or requires Parties to provide a legal basis for requests;
— this article requires that the request emanate from a competent authority;
— this Protocol provides that a request is made for the purposes of specific criminal investigations or proceedings;
— this article requires that the request contain a statement that the need for the information arises because of its relevance to a specific criminal investigation or proceeding and that the information will only be used for that specific criminal investigation or proceeding;
— this Protocol provides for safeguards for the processing of personal data disclosed and transferred pursuant to such requests through Article 14;
— the information to be disclosed is limited and would not permit precise conclusions to be drawn concerning the private lives of individuals;
— entities may be expected or required to co-operate under contractual arrangements with ICANN.
Interplay with System of Standardized Access/Disclosure model:

- Hope is that this Article will work with ICANN SSAD
- Not clear (yet) how the interplay will work
- T-CY may have to work with ICANN going forward

Benefits:

- Complements ICANN multi-stakeholder policy for criminal investigations
- Provides safeguards that should facilitate the ability of registrars to respond
- Hopefully provides an effective and efficient framework to obtain information for identifying or contacting the registrant of a domain name
2nd Additional Protocol to the Convention on Cybercrime: benefits

Operational value:

- Basis for direct cooperation with service providers for subscriber information ("direct disclosure")
- Effective means to obtain subscriber information and traffic data ("giving effect")
- Legal basis for disclosure of WHOIS information
- Cooperation in emergencies ("expedited disclosure" + "emergency MLA")
- Mutual assistance tools ("video-conferencing", "JITs")
- Data protection safeguards to permit the flow of personal data under the Protocol

Policy value:

- Convention on Cybercrime will remain relevant and effective
- Efficient cooperation with rule of law and data protection safeguards is feasible
- Respect for free Internet with limited restrictions in case of criminal misuse (specific criminal investigations, specified data)
Part 2

Panel Discussion
Questions

- Is there an expectation that ICANN (both community and organization) should respond to these developments?
  - How should the ICANN community respond?
  - What are alternative paths?

- How should the ICANN multistakeholder model take into account legislative and regulatory proposals that could have an impact on ICANN policies and the DNS, such as the examples highlighted in this session?

- What lessons have we learned from experience, and how can we be better prepared in the future?
Part 3

Community Discussion
One World, One Internet

Visit us at icann.org

@icann
facebook.com/icannorg
youtube.com/icannnews
flickr.com/icann
linkedin/company/icann
soundcloud/icann
instagram.com/icannorg