STRUCTURING CRITERIA FOR ADDRESSING COVID-19 RELATED ABUSE AT DNS LEVEL

REF: 20-105 | April 23, 2020

As with other emergencies (natural disasters, terrorist incidents), the COVID-19 pandemic has given rise to opportunism and activities spreading misinformation and fraud (including through spam or phishing).

Action at the level of the Domain Name System (DNS) is always a blunt tool: it has a global impact and is not specific enough to limit access to individual pieces of content. Moreover, the underlying site connected to a blocked domain name remains accessible through the server's IP address. Actors other than DNS operators, including hosting providers, are often able to provide a more proportionate response. Action at the DNS level is thus justified only if a particularly high threshold of abusive activity or content is met.

Accordingly, in the context of the COVID-19 crisis, some DNS Operators may choose to take action on a voluntary basis to address fraud and abuse when it poses an imminent threat to public health, through an expedited workflow, including some exceptional proactive monitoring of recent registrations. In all cases, close coordination with local law enforcement authorities remains essential.

The Internet & Jurisdiction Policy Network[1] and its three Programs[2] have for more than five years facilitated discussions among public, private and civil society actors on jurisdictional internet challenges, in particular **DNS-level action to address abuse**. This extensive experience demonstrates the importance of a **common frame of reference** among actors to properly address an issue, design solutions and evaluate their impact.

In that spirit, this **Framing Brief from the I&JPN Secretariat**, building on interactions with Policy Network members, presents common framing and analytic criteria regarding acting at the DNS level in this exceptional circumstance. It aims to assist various stakeholders as they consider this issue.

Questions are structured around five major themes: **Justification for such exceptional action**, and the four stages of decision-making: ***Identification, Evaluation, Action and Recourse***. We hope that this list will help trigger meaningful discussions on a shared basis.

Sharing of identified initiatives with the I&JPN Secretariat is strongly encouraged. Please send relevant information to: <secretariat[at]internetjurisdiction.net> with this reference in the subject line: #20-105

STRUCTURING CRITERIA

I. JUSTIFICATION FOR EXCEPTIONAL ACTION

- **Threshold:** Does "manifest imminent threat to public health" represent a proper basis for action?
- **Terms of Service:** Do the Operator's Terms of Service already permit action to address such threat or do they need to be specifically adapted?
- **Temporality:** How long are the exceptional measures and any resulting action supposed to remain in place, and does this potentially establish a precedent?

II. IDENTIFICATION

At present, there is no established Reputation Block List to independently identify domains used in COVID-19 related misinformation/fraud. Thus, proactively identifying potentially problematic domains falls largely to DNS operators.

[1] https://www.internetjurisdiction.net/

[2] https://www.internetjurisdiction.net/work

- **Scope:** What is the period covered (e.g. does it cover only domains recently registered)?
- **Detection:** How extensive are the search terms (e.g. "corona", "covid", "cure', "test") to identify potentially problematic domains in a DNS zone file?
- **Frequency:** How regularly is the zone file queried?
- **Case matching:** What is the level of keyword case matching that is used (e.g. exact match, typographic variations, combinations)?
- **Updating:** How frequently are search terms revised?
- **Third party notifiers:** What is their potential role?

III. EVALUATION

What questions can assist Operators to evaluate whether to take action?

- **Resolving:** Does the registration data indicate a name server configuration?
- **Parking:** Is the domain parked?
- **Manifestly inappropriate content:** Does a prima facie analysis establish the abuse beyond a sufficient threshold (e.g. promoting a cure or vaccine; asking for money/enabled shopping cart?)
- **Malware distribution or phishing:** Is there sufficient evidence (e.g. download function; personal data collection)?
- **Economic Impact:** Would price gouging or misinformation without economic fraud meet the threshold?
- **Referral:** If the DNS operator feels unable to fully complete the evaluation on its own, what third party experts (law enforcement, regulatory bodies, courts, internet intermediaries, others) could provide additional evaluation?

IV. ACTION

What is the appropriate action to remediate the abuse?

- **Should Manifest bad faith activity posing imminent threat result in:**
  - Referral to local authorities and/or internet intermediaries?
  - Locking, suspending and/or redirecting the domain?
- **Notice to registrant:** Ex-ante or Ex-post?
- **In case of questionable, but not manifest evidence of bad faith posing imminent threat to public health, should Operator:**
  - Refer to local authorities and/or internet intermediaries?

V. RECOURSE

Once action has been taken, what recourse mechanisms are available for aggrieved registrants?

- **Operator initiated action**
  - Appeal directly to Operators via Abuse POC?
  - Other?
- **Action taken pursuant to court order from Operator's place of jurisdiction**
  - Appeal to the court that issued the order?
- **Transparency Reporting Requirements:**
  - When, how frequently and to whom should the Operator disclose information concerning its actions?

Although some operators may choose to exceptionally take voluntary proactive measures, addressing COVID-19 related abuse remains a shared responsibility among diverse actors, such that it does not lie solely with Operators. Regular and ongoing coordination with law enforcement and other public authorities is necessary to ensure that the action taken is appropriate and proportionate.