INTERNET & JURISDICTION POLICY NETWORK

# DOMAINS & JURISDICTION

## WORK PLAN

*This Work Plan was reviewed and refined by stakeholders gathered on February 26-28, 2018 in Ottawa, Canada for the 2nd Global Conference of the Internet & Jurisdiction Policy Network. Taking stock of the outcomes of the 1st Global Conference in 2016 in Paris, and the intersessional work conducted in 2017, this document will guide the work in the Domains & Jurisdiction Program of the Policy Network in preparation for its 3rd Global Conference, which will take place in Berlin, Germany, on June 3-5, 2019.*

Cross-border requests for domain name suspension are increasingly sent to technical operators in relation to the alleged abusive content or activity on underlying websites[1].

Yet, the DNS, as an addressing system, is a neutral technical layer vital for the proper functioning of the internet. This level is neither a fully effective way - nor should be considered as the natural tool - to address abusive content. Protection of the core of the Internet is and should be a key priority.

Acting at the DNS level should only be considered when it can be reliably determined that the domain itself is used with a clear intent of significant abusive conduct. Furthermore, because a domain suspension has by definition a global impact, proportionality imposes that only a particularly high level of abuse and/or harm could potentially justify resorting to such a measure. It is important that the impact of a specific action at DNS level is well understood.

This important issue is generally recognized as outside of ICANN's mandate. Moreover, the fundamental distinctions between country-code and generic Top Level Domains in terms of relations with, respectively, ICANN and national laws or authorities, lead to very different approaches and constraints.

All actors are nonetheless confronted with a common challenge: defining when is it appropriate to act at the DNS level in relation to the content of a site and what role courts and so-called "notifiers" should or could respectively play.

[1] This exercise focuses on abusive content, not registration or infrastructure abuse.

## Objective

In this perspective, participants in the Domains & Jurisdiction Workstream at the second Global Conference of the Internet and Jurisdiction Policy Network in Ottawa, Canada, on February 26-28, 2018, identified as a common objective to define, on a topic-by-topic basis:

- Under what strict conditions suspension of a domain name without consent of the registrant be envisaged/acceptable,
- What actions should/would domain name operators be willing and able to exercise;
- What rules and procedures could help establish or enhance the credibility of notifiers' notifications (for information or action); and
- What possible mechanisms can help improve transparency in such processes.

## Structuring questions

Accordingly, further discussions to be facilitated by the Secretariat of the Internet & Jurisdiction Policy Network in the perspective of its third Global Conference in Berlin on June 3-5, 2019 will be organized around the following structuring questions, on a topic-by-topic basis:

1. **Standards**: Taxonomy and threshold levels for action relevant to each type of abusive behavior and content.
2. **Court orders**: The role of court orders, their territorial reach, their effectiveness regarding their purpose, and their proportionality.
3. **Notification**: Criteria relevant to evaluate the credibility of a notification, the source (i.e. the notifier) being only one element.
4. **Due Diligence**: The procedures notifiers should ideally follow before sending out notifications, and the content of their requests.
5. **Procedural guarantees**: Protections for registrants (notification and contradictory procedure, proportionality)
6. **Remediation**: Appeal mechanisms and technical precautions allowing for remediation.
7. **Request validation**: Options for certification of notifications.
8. **Liability**: Potential protections for operators when proper due diligence is conducted.
9. **Transparency**: Mechanisms to ensure appropriate transparency, including in relation to how operators deal with notifications; and how notifiers ensure due process prior to notification.
10. **Education**: Accessible and good quality information for lawmakers, courts and law enforcement to prevent unintended consequences of decisions, as well as for end users, who can play a crucial role in preventing abuse to happen/be effective.
11. **Tools**: Software and/or processes to enable effective, proportionate and scalable measures.