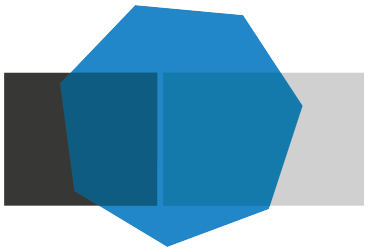


INTERNET
& JURISDICTION
POLICY NETWORK

DOMAINS & JURISDICTION POLICY OPTIONS

CROSS-BORDER DOMAIN SUSPENSION

November 2017

Input Document for Workstream III of the second Global Internet and Jurisdiction Conference

GLOBAL INTERNET
AND JURISDICTION
CONFERENCE 2018
FEBRUARY 26-28 • OTTAWA, CANADA
conference.internetjurisdiction.net

@IJurisdiction
www.internetjurisdiction.net

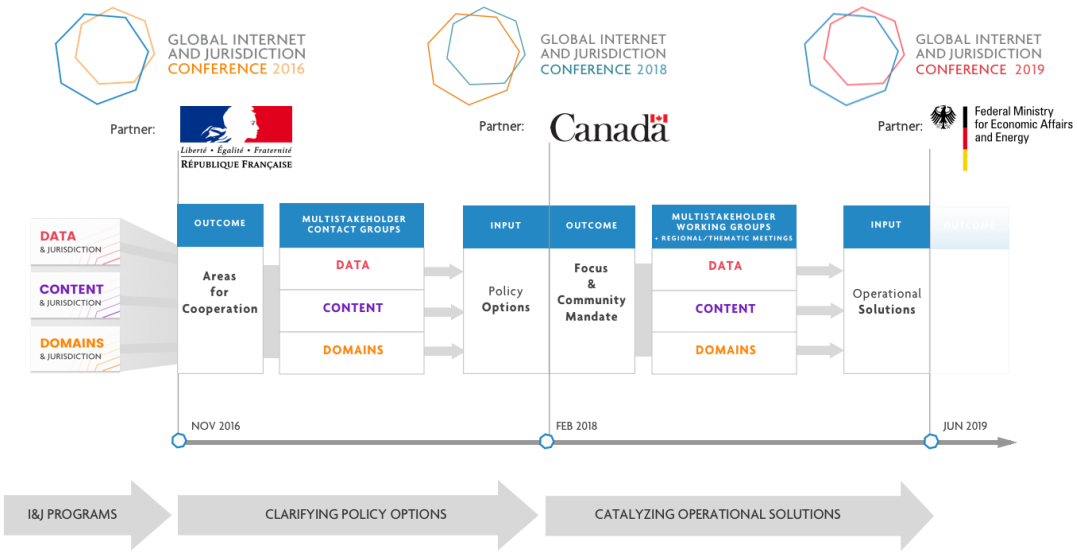
This Policy Options document prepared by the Secretariat of the Internet & Jurisdiction Policy Network presents the results of the work of the multistakeholder Domains & Jurisdiction Contact Group. This Group was set up as a result of the first Global Internet and Jurisdiction Conference of the Policy Network[1], held in Paris on November 14-16, 2016, and which gathered 200 senior-level participants from 40 countries. The Group held seven virtual meetings in 2017 to explore the Areas of Cooperation identified in Paris (see Domains & Jurisdiction Framing Paper[2]).

Reflecting preparatory work, this document will serve as input to structure discussions in Workstream III on Domains & Jurisdiction on Day 2 of the second Global Internet and Jurisdiction Conference[3] in Ottawa on February 26-28, 2018. On this basis, stakeholders are expected to agree there on focus and community mandates to structure further work in the Internet & Jurisdiction Policy Network.

Feedback on this document can be submitted to the Secretariat until January 26, 2018 via gijc2018-domains@internetjurisdiction.net. It will be shared with the Members of the Contact Group.

AN ONGOING PROCESS TOWARDS OPERATIONAL SOLUTIONS

The second Global Internet and Jurisdiction Conference of the Internet & Jurisdiction Policy Network is organized in partnership with the Government of Canada, and institutionally supported by OECD, UNESCO, Council of Europe, European Commission, and ICANN. It will be a milestone moment to identify concrete focus and priorities to develop operational solutions to major jurisdictional challenges. This will define the methodology and roadmap in the lead-up to the third Global Internet and Jurisdiction Conference in June 2019, which will be organized in partnership with the Government of Germany.



ABOUT THE DOMAINS & JURISDICTION CONTACT GROUP

The Contact Group was set up under the Domains & Jurisdiction Program of the Internet & Jurisdiction Policy Network. Parallel Contact Groups have been set up in the Data & Jurisdiction and Content & Jurisdiction Programs, as well. The Group is composed of Members of different stakeholder constituencies, actively involved in addressing the jurisdictional challenges related to abusive use of the Domain Name System. This neutral space allowed participants to map their respective perspectives, compare approaches, foster policy coherence, and identify possible steps for coordinated actions.

---

[1] See: https://conference2016.internetjurisdiction.net
[2] Secretariat of the Internet & Jurisdiction Policy Network (2017). Framing Paper of the Domains & Jurisdiction Program https://www.internetjurisdiction.net/publications/paper/domains-jurisdiction-program-paper
[3] https://conference.internetjurisdiction.net

Members of the Contact Group are:

- **Benedict Addis**
  Chair
  Registrar of Last Resort (RoLR)
- **Maarten Botterman**
  Board Member
  Internet Corporation for Assigned Names and Numbers (ICANN)
- **Edmon Chung**
  CEO
  DotAsia Organisation
- **Keith Drazek**
  Vice President
  Public Policy and Government Relations
  VeriSign
- **Hartmut Glaser**
  Executive Secretary
  Brazilian Internet Steering Committee (CGI.br)
  Brazil
- **Byron Holland**
  President and CEO
  Canadian Internet Registry Authority (CIRA)
- **Paul Mitchell**
  Senior Director Tech Policy
  Microsoft
- **Alice Munyua**
  Founder
  Kenya ICT Action Network (KICTANet)
- **Richard Plater**
  Policy Executive
  Nominet
- **Peter Van Roste**
  General Manager
  Council of European National Top-Level Domain Registries (CENTR)
- **Fiona Alexander**
  Associate Administrator
  United States Department of Commerce NTIA
- **Mark Carvell**
  Senior Policy Adviser, Global Internet Governance Policy
  Department for Culture, Media and Sport,
  United Kingdom
- **Mason Cole**
  Vice President,
  Communications and Industry Relations, Donuts
- **Elizabeth Behsudi**
  Vice President and General Counsel
  Public Interest Registry
- **Jamie Hedlund**
  Vice President, Contractual Compliance and Consumer Safeguards
  Internet Corporation for Assigned Names and Numbers (ICANN)
- **Désirée Miloshevic**
  Senior Public Policy and International Affairs Advisor
  Afilias
- **Cristina Monti**
  Head of Sector, Internet Governance and Stakeholders' Engagement, European Commission
- **Michele Neylon**
  CEO
  Blacknight Internet Solutions
- **Rod Rasmussen**
  Co-chair
  Anti-Phishing Working Group (APWG)
- **Thomas Schneider**
  Ambassador, Director of International Affairs
  Federal Office of Communications (OFCOM),
  Switzerland

ABOUT THE INTERNET & JURISDICTION POLICY NETWORK

The Internet & Jurisdiction Policy Network addresses the tension between the cross-border nature of the internet and national jurisdictions. Its Paris-based Secretariat facilitates a global multistakeholder process to enable transnational cooperation. Participants in the Policy Network work together to preserve the cross-border nature of the Internet, protect human rights, fight abuses, and enable the global digital economy. Since 2012, the Internet & Jurisdiction Policy Network has engaged more than 200 key entities from governments, Internet companies, technical operators, civil society, academia and international organizations around the world. Its Secretariat has convened, organized or contributed to more than 120 policy events in over 30 countries.

Domains & Jurisdiction Policy Options

This document aims at providing, in a forward-looking approach, guiding elements for further discussion at the second Global Internet and Jurisdiction Conference in Ottawa in February 2018 and beyond. It explores inter alia the due process dimensions of voluntary regimes envisaged by some DNS operators to deal with domain takedown requests and the potential role of so-called "notifiers". Although such voluntary approaches are not supported by all stakeholders and even opposed by some, this should provide a helpful contribution to these discussions.

Trust in the Domain Name System (DNS) is critical to the functioning of the global internet. Protecting the neutrality of this technical layer vis-à-vis political or commercial pressure is a key factor in that regard. However, given the difficulty of dealing with a diversity of online abuses across borders, pressure is mounting to leverage domain names to address the illegality of content or activities on the underlying sites[4].

Registries and registrars are very diverse in terms of size, activities, governance structures and practices. More importantly, 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. Nevertheless, all these actors are confronted with similar challenges and pressures.

There is a traditional distinction between registration abuse and *use abuse*[5]. This document focuses on use abuse, where little clarity exists on whether an action at the level of a domain name should be taken in relation to an activity or content on the underlying site.

On a principle level, in light of the neutral function of the DNS and the overarching norm of proportionality, the fact that a domain suspension has, by nature, a global impact calls for a particularly high threshold of abusive activity or content to justify such a measure. Furthermore, a fundamental first criterion to take into account is the actual involvement and intent of the registrant itself in the infringing behavior or content. Finally, irrespective of harm types, blocking at the DNS level can have limited efficiency in preventing users from getting access to the resource they want to reach.

In this context, discussions in the Contact Group explored both *infrastructure abuse* and *abusive content*, with a particular focus in the latter case on the increasing role that specialized notifiers try to play and the conditions under which sufficient due process guarantees can be established.

---

[4] See the I&J Domains & Jurisdiction Framing Paper released after the first Global Internet and Jurisdiction Conference held in Paris in November 2016: https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Paper.pdf

[5] See the report from the ICANN GNSO Registration Abuse Policies Working Group (RAPWG): https://gnso.icann.org/en/issues/rap/rap-wg-final-report-29may10-en.pdf

1. Infrastructure abuse

Infrastructure abuse (e.g. phishing, malware distribution, botnet support), being closely related to security and stability of the DNS, does justify appropriate action by registries and registrars, albeit with caution when otherwise legitimate sites have been compromised. Formal and informal cooperation efforts to detect, report and mitigate such abuses should be further developed. Within its specific remit, ICANN can play a role in that regard, though not an exclusive one, taking also into account in the important differences between ccTLDs and gTLDs.

2. Abusive content

How to deal with abusive content (e.g. child sexual abuse imagery, inappropriate online sale of pharmaceuticals[6], counterfeiting and copyright infringement) is more debated. There is general agreement that this falls outside of ICANN's mandate[7], but that these topics deserve further discussions among all stakeholders.

The DNS is only an addressing system. When a domain name is deleted, the online content can remain available to those wanting to access it (e.g. via the IP address). The DNS level is therefore not an effective way to address abusive content. This instrument is also too blunt, as most forms of abuse on the internet occur on domains compromised in some way, or via a legitimate service being taken advantage of for abusive purposes. Regardless of the type of abusive content, acting at the DNS level should therefore only be considered appropriate when it can be reliably determined that the domain itself is registered with the express intent of significant abusive conduct. Remedial action should then be conducted with strict procedural safeguards.

DNS operators should not be responsible for actively policing their space, nor for being the judge of complex legal determinations and attach great importance to keeping the freedom to choose which abuses and notifications they act upon. In this context, fear of slippery slopes often hold them back in their desire to deal with alleged abuses:

- Voluntarily committing to deal with certain types of abuse can open a Pandora's box, putting a strain on operators' usually limited resources,
- This can result in greater liability down the road for failure to act or for unjustified takedowns,
- If voluntary commitments end up working well, it could later encourage the mandatory inclusion of such measures in accreditation agreements for gTLDs.

For the sake of legal certainty and limitation of liability, operators often prefer to simply have to comply with authoritative decisions.

---

[6] A distinction here needs to be made between "substandard or falsified medical products" and licensing/trademark disputes (see WHO terminology at: http://www.who.int/medicines/regulation/ssffc/definitions/en/)

[7] Links to positions by the ICANN Board and staff are in the annexes in the Domains & Jurisdiction Framing Paper (see endnote 1)

3. Court orders

In that respect, court orders provide two advantages: procedural guarantees and clarity of applicable law. Operators generally only obey - and usually even demand - orders from legal entities from the country in which they are located, wary that accepting foreign court orders would incentivize governments to exercise extraterritorial authority in an unpredictable manner.

However, any national court decision regarding a domain name, if implemented, unfortunately can imply imposing the legislation of one particular country over registrants, activities and users around the world[8]. This confers strong power to countries where many operators are located. It also raises jurisdictional questions regarding cross-border enforceability of law(s).

In this context, a diversity of self-established specialized "notifiers[9]" are documenting perceived abuses and proposing formal agreements to operators. Their credibility, track record and the procedural guarantees they implement should determine their relevance.

4. Credibility of notifiers

Notifiers are self-established entities, of various sorts and structures. Some of them have formal agreements with operators, but no external "accreditation" mechanism exists to certify their credibility and they only have the authority that operators accept to bestow upon them.

Operators can use various factors to decide whether to enter into an agreement with a notifier or accept its requests, including its structure and governance framework, the explicit criteria and legal basis (national or more general) upon which its evaluations are based, its neutrality and potential conflicts of interest, and the procedural guarantees it provides.

The overarching criterion however is reputation over time: how long the notifier has been active, its track record on the market and, more importantly, whether it is willing to defend its notices and stand by the operator in case of litigation.

5. Due Diligence

Analysis of current practices by operators help identify important components of good requests by notifiers, including:

- Credentials of the requesting entity,
- Activity conducted and methodology for analysis,
- Alleged abuse and why it is appropriate to be dealt with according to the requester,
- Specific action requested - coming from an agreed-upon list of specific actions,
- Procedure followed by the requester to come to this determination,
- Clear authority to mandate such action.

---

[8] The different situation between ccTLDs and gTLDs is important in this regard

[9] A (non-exhaustive) list of such notifiers was provided in the Domains & Jurisdiction Framing Paper

However, the more detailed the notifications are, the more operators are obliged to make determinations on topics or legal issues they do not have competence in. Some mechanism would therefore be preferred, whereby notifiers would guarantee that proper due diligence has been conducted on each notice, according to an agreed list of criteria and procedures.

6. Substantive norms

Discussions showed strong agreement on approaches regarding infrastructure abuse and child sexual abuse imagery. They highlighted however the absence of commonly agreed norms regarding the threshold beyond which other types of abusive content should be tackled, if at all.

Further interactions are needed, on a topic-by-topic basis and involving inter alia the most relevant notifiers, to clarify how appropriate criteria can be developed in that regard.

7. Procedural guarantees

Beyond detailed substantive criteria analysis by notifiers, due process guarantees are essential. They include in particular notification of the registrant and a contradictory procedure before action is taken, except in duly justified conditions of emergency.

Clear standards and proper mechanisms for appeal and redress are also necessary.

8. Liability

Explicit mention in operators' Terms of Service of an agreement with a particular notifier would both inform registrants and provide some protection from liability to the operators. In particular, liability for damages could be excluded when an operator follows the request of a trusted notifier and courts should be encouraged to recognize this.

Overall, the more due process standards are documented, the more operators' liability can be reduced. Notifiers also have an interest in developing due process to reduce their own liability.

9. Policy options

Even within the above concept of notices certified for due diligence, operators still can choose the issues they accept to handle and the notifiers they sign an agreement with, if any, as well as retain the capacity to ultimately accept or refuse such notifications, within the context of applicable law(s).

Certification of notices can be implemented in different ways, including the following options:

1) The notifier itself develops its due process guarantees, ensuring registrant notification, contradictory procedures, appeal and redress. Related questions are: How to ensure the neutrality of the notifier and address the fact that it might become judge and party? Should some functional separation be envisaged inside these structures? Can third party audits provide some oversight?

2) A third party accredits the notifier as a whole, on the basis of an evaluation of the quality of its substantive and procedural standards, and its notifications are accordingly considered as trusted. A natural question here is: who can play the role of such a third party accreditor[10] and what review mechanisms should then be put in place?

3) Some third party implements the due process guarantees and certifies each notification after full weighing of the evidence. Such third party could also receive and treat general notifications by a wider range of individuals and entities. While this provides more protection, it also can make the process heavier and slower. Related questions are: How and by whom could such mechanisms be established and their independence guaranteed?

These different options are not necessarily strictly alternative, nor limitative. Different solutions could also apply to different types of abuses, according to the degree of harm and urgency they entail. Coordinated evaluations by a critical mass of major operators could also facilitate joint evaluation of notifiers' credibility.

10. Further discussions

In light of the Contact Group exchanges, the following issues could structure further discussions in the perspective of the second Global Internet and Jurisdiction Conference and the follow-up work:

- Clarification of best practices for transparency reporting. Pressure for transparency will develop and operators have an interest in a proactive move in that regard,
- Clarification of substantive threshold criteria on a topic-by-topic basis for the different types of abusive content,
- Clarification of due process guarantees and mechanisms, including appeal and redress,
- Examination of the different options for validation of notifications.

Some of this work can be conducted by side initiatives, updating the Secretariat of the Internet & Jurisdiction Policy Network on progress, while other aspects will remain the focus of the Data & Jurisdiction Program.

[10] ICANN plays such a role in the accreditation of UDRP dispute providers. This is only mentioned as an analogy: ICANN is clearly not considered an appropriate certifier for content related issues.