INTERNET
& JURISDICTION
A GLOBAL MULTISTAKEHOLDER
POLICY NETWORK

DOMAINS & JURISDICTION PROGRAM:

CROSS-BORDER DOMAIN SUSPENSION

Problem Framing
May 2017

@IJurisdiction
www.internetjurisdiction.net

ABOUT
INTERNET & JURISDICTION

Internet & Jurisdiction is the global multistakeholder policy network addressing the tension between the cross-border Internet and national jurisdictions. It facilitates a global policy process to enable transnational cooperation and preserve the global character of the Internet. Founded in 2012, the policy network engages key entities from different stakeholder groups around the world.

Internet & Jurisdiction helps catalyze the development of shared cooperation frameworks and policy standards that are as transnational as the Internet itself in order to promote legal interoperability and establish due process across borders.

INTERNET
& JURISDICTION

14 rue Alexandre Parodi
75010 Paris, France
www.internetjurisdiction.net

DOMAINS & JURISDICTION

After five years of exchanges in the Internet & Jurisdiction policy network, three concrete issue areas were collectively identified as priority fields for action: cross-border requests for access to user data, content takedowns, and domain suspensions. Transnational due process mechanisms are necessary in each case. In early 2016, Internet & Jurisdiction launched its first series of thematic programs to better hone, structure, and support the corresponding activities of the I&J process. Based on the 2016 Global Internet and Jurisdiction Conference, this document presents a general framing of the DOMAINS & JURISDICTION program.

DOMAINS &
JURISDICTION

How can the neutrality of the internet's technical layer be preserved when national laws are applied on the Domain Name System?

Cross-border domain name suspension requests are increasingly sent to technical operators based on the content or activity of underlying websites. Such measures have global impact by nature and therefore require strong procedural guarantees to ensure proportionality and respect of the neutrality of this technical layer. Common vernacular must also be agreed upon between the technical and policymaking communities to permit fruitful discussions. What are the criteria for abuses that can justify domain suspension, and how can the transparency of such requests be increased?

A TRANSBORDER CHALLENGE

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.

ICANN's GNSO’s Registration Abuse Policies Working Group (RAPWG) in 2010 identified a key distinction between Registration Abuse and Use Abuse. An ICANN report in July 2016 reiterated the RAPWG position "that ICANN and its various supporting organizations have some purview over registration issues through the policy-making and enforcement processes, while use issues are more difficult to confront given ICANN’s limited authority over how registrants use their domain names.”

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 underlying content or activities. Two different types of use abuses are invoked in that regard:

- Abuses leveraging the DNS itself, such as phishing, diffusion of malware, or support for botnets;
- Site content or activity that is considered illegal or harmful, including distribution of child abuse images, illegal online pharmaceutical sales, counterfeiting or copyright infringement.

Both situations present strong transnational dimensions, involving operators, domain holders and users in multiple jurisdictions. Determining applicable law(s) and enforcing national court decisions is therefore difficult and extensive cross-border cooperation is often necessary. The problem is compounded when the site content or activity is legitimate in some countries but deemed illegal in others, or when only a minor portion of the content or activity is considered illegal.

NEED FOR STANDARDS AND PROCEDURES

Given the global impact of a domain name suspension, it can only be justified in relation to the underlying site if a very high threshold of illegal or objectionable activity is met. Yet, registries and registrars receive more and more of such requests, coming from inside or outside their country of incorporation, with or without court orders. This situation presents several challenges, including:

- **Proportionality.** Domain suspension can easily be a disproportionate measure if only a portion of the content is objected to or if content is deemed illegal only in certain countries. Furthermore, domain names are used for many services - for instance email addresses - that are subsequently impacted by a suspension. In any case, an objectionable website remains accessible via its IP address even if its domain is suspended.
- **Burden shift.** Increasing responsibilities are being put on private technical operators to decide difficult legal issues without sufficient competence or guarantees of due process. Furthermore, in spite of their global reach, many DNS operators remain small actors with very limited human and financial resources that struggle to evaluate the validity of these requests.
- **Extraterritorial impact.** National authorities' actions on operators based within their borders can have extraterritorial impact on registrants based in other countries even when they conduct activities that are fully legal in their own jurisdiction. Conversely, operators usually accept to comply only with decisions from courts in their country of incorporation, thus imposing the law of that country upon content or activity in other jurisdictions.
- **Negative incentives.** The operators' limited resources can incentivize them to accept requests in order to avoid liability. Meanwhile, the lack of agreed-upon global mechanisms encourages blocking measures at the national level and even requirements for operators to register in a particular country in order to serve users there.
- **Economic impact.** Limiting the capacity to register domain names from anywhere in the world would potentially affect the level playing field for competition and harm developing countries.

Transnational procedures and criteria need to be developed to maintain the neutrality of the Internet's technical layer and guarantee due process while dealing with abuses.

A TRANSBORDER CHALLENGE

Enforcing court decisions across borders is a complex and lengthy process and national legislations remain highly disparate. In this context, the development of more transnational procedures and decision-making criteria is hampered by disagreement on where such discussions should take place. The key approaches are:

An ICANN-based policy approach. Some actors consider that dealing with illegal content on sites under a domain name is (or should be considered as) covered by the obligations contained in the accreditation contracts that registries and registrars sign with ICANN. In this view, ICANN's compliance department should enforce these provisions more systematically and the presence of all relevant actors in the multistakeholder ICANN community make it the natural place to develop any additional policy deemed necessary.

On the other hand, ICANN and its Board of Directors contend that this would far exceed ICANN's limited mandate, particularly in the context of the revised Bylaws after the IANA Transition. They maintain that ICANN, as the technical coordinator of the system of identifiers, should not be involved in policing underlying content. Furthermore, ICANN has no authority on Country-Code Top Level Domains (ccTLDs) that are also confronted with these challenges.

In any case, a full policy development process (PDP) would be lengthy at best and even potentially deadlocked given the diversity of positions within the community. It is also argued that some relevant stakeholders are insufficiently represented in the ICANN community for a PDP to be appropriate.

An industry-led voluntary regime. In early 2016, the Domain Name Association (DNA), a business association representing certain interests of the domain name industry, launched a voluntary approach to self-regulation called the Healthy Domains Initiative (HDI). This initiative is intended to help develop, among other things, "more effective methods of addressing abuse complaints in the internet community" regarding online abuse, rogue pharma, child abuse imagery, and copyright infringement. In February 2017, the DNA released 30 “healthy practices” related to the three first issues.

However, a disparity of positions remains within the industry itself concerning such self-regulatory approaches, as evidenced by debates in early 2017 regarding initial recommendations related to copyright[1]. Several actors within the ICANN and law enforcement communities furthermore consider that the public interest dimension of these issues demand that they be discussed by a broader range of actors than just the private operators. Some even oppose the very approach of industry self-regulation, or at least highlight the need for stronger guarantees of due process to prevent the risk of excessive suspensions.

Tensions around these two approaches tend to prevent a constructive discussion on substance.

ROLE OF NOTIFIERS

Irrespective of where and how such discussions should take place, the growing role of third-party notifiers in flagging domains for suspension based on illegal or offensive content has become a recent and growing trend. On issues as diverse as child sexual abuse images, phishing, online pharmacies, counterfeiting, or copyright, national or international networks of associations have taken it upon themselves to proactively or reactively identify alleged abuses and report them to DNS operators.

Such mechanisms are presented as a way to alleviate the burden on operators to make judgments in these situations and several technical operators have made formal or informal arrangements with such notifiers.

However, evaluations by notifiers are often established without sufficiently clear procedures or mechanisms for redress and may be based on the laws of only one particular country or the interests of trade associations. Furthermore, their structure, governance and redress mechanisms greatly vary and strongly determine the level of trust bestowed upon them.

Transparency and accountability frameworks for such notification schemes therefore constitute a key topic requiring further discussion.

[1] Following stakeholder feedback in February 2017, the DNA announced its intention to further study and consider 7 proposals made related to alternate dispute resolution for copyright claims. Recommendations in other issue-areas remained unchanged.

AREAS OF COOPERATION

The first Global Internet and Jurisdiction Conference, held in Paris on November 14-16, 2016, gathered more than 200 senior representatives from the different stakeholder groups in the I&J Policy Network. Exchanges conducted there and in the following months on this issue helped identify a limited list of "areas of cooperation" and the following concrete questions to structure further discussions.

1. COMMON TERMINOLOGY

1.1 How should the different types of abuses be labeled?

1.2 How can a shared wording be developed for potential technical responses to abuses?

1.3 How can the various types of notifiers be categorized?

1.4 What are the types of actors and their "capacity to act"?

2. DECISION-MAKING CRITERIA

2.1. How can the appropriate response for each type of abuse be determined?

2.2. Which criteria should determine applicable law(s) and the validity of court orders – location of the registry, the registrar, the domain holder, the country where the underlying activity or content is deemed infringing, etc.?

3. ROLE AND ACCOUNTABILITY OF NOTIFIERS

3.1. Which criteria should determine notifier credibility – nature of the individual/organization, legal basis for evaluations, type of abuse, internal procedures, governance, etc.?

3.2. How can accountability and due process be ensured? (Monitoring of accuracy, oversight, dispute mechanisms, redress mechanisms, etc.)

4. TRANSPARENCY AND FORMATS

4.1. How can standards be developed for reporting on requests?

4.2. How can a standard be developed regarding the core elements that requests should contain?

RESOURCES

APPROACHES

ICANN

Reaffirmation of ICANN's limited mandate:

Letter from Board Chair Steve Crocker (June 2016)

> "This does not mean, however, that ICANN is required or qualified to make factual and legal determinations as to whether a Registered Name Holder or a website operator is violating applicable laws and governmental regulations, and to assess what would constitute an appropriate remedy for such activities in any particular situation."

https://www.icann.org/en/system/files/correspondence/crocker-to-shatan-30jun16-en.pdf

Post by Allen Grogan, ICANN Chief Contract Compliance Officer (June 2015)

> "Allow me to say this clearly and succinctly – ICANN is not a global regulator of Internet content, nor should the 2013 Registry Accreditation Agreement (RAA) be interpreted in such a way as to put us in that role. Our mission is to coordinate, at the overall level, the global Internet's systems of unique identifiers, and in particular, to ensure the stable and secure operation of the Internet's unique identifiers. ICANN was never granted, nor was it ever intended that ICANN be granted, the authority to act as a regulator of Internet content."

https://www.icann.org/news/blog/icann-is-not-the-internet-content-police

Registry Agreement (under Specification 6)

> 4.1. Abuse Contact. Registry Operator shall provide to ICANN and publish on its website its accurate contact details including a valid email and mailing address as well as a primary contact for handling inquiries related to malicious conduct in the TLD, and will provide ICANN with prompt notice of any changes to such contact details.

https://www.icann.org/news/blog/icann-is-not-the-internet-content-police

Registrar Accreditation Agreement (under 3.18, "Registrar's Abuse Contact and Duty to Investigate Reports of Abuse)

> **3.18.1** – Registrar shall maintain an abuse contact to receive reports of abuse involving Registered Names sponsored by Registrar, including reports of Illegal Activity. Registrar shall publish an email address to receive such reports on the homepage of Registrar's website (or in another standardized place that may be designated by ICANN from time to time). Registrar shall take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse.
>
> **3.18.2** – Registrar shall establish and maintain a dedicated abuse point of contact, including a dedicated email address and telephone number that is monitored 24 hours a day, seven days a week, to receive reports of Illegal Activity by law enforcement, consumer protection, quasi-governmental or

other similar authorities designated from time to time by the national or territorial government of the jurisdiction in which the Registrar is established or maintains a physical office. Well-founded reports of Illegal Activity submitted to these contacts must be reviewed within 24 hours by an individual who is empowered by Registrar to take necessary and appropriate actions in response to the report. In responding to any such reports, Registrar will not be required to take any action in contravention of applicable law.

3.18.3 – Registrar shall publish on its website a description of its procedures for the receipt, handling, and tracking of abuse reports. Registrar shall document its receipt of and response to all such reports. Registrar shall maintain the records related to such reports for the shorter of two (2) years or the longest period permitted by applicable law, and during such period, shall provide such records to ICANN upon reasonable notice.

https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en

New gTLD Accreditation Agreement (under Specification 11, Section 3a and 3b)

3. – Registry Operator agrees to perform the following specific public interest commitments, which commitments shall be enforceable by ICANN and through the PICDRP. Registry Operator shall comply with the PICDRP. Registry Operator agrees to implement and adhere to any remedies ICANN imposes (which may include any reasonable remedy, including for the avoidance of doubt, the termination of the Registry Agreement pursuant to Section 4.3(e) of the Agreement) following a determination by any PICDRP panel and to be bound by any such determination.

3a. – Registry Operator will include a provision in its Registry-Registrar Agreement that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name.

3b. – Registry Operator will periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. Registry Operator will maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. Registry Operator will maintain these reports for the term of the Agreement unless a shorter period is required by law or approved by ICANN, and will provide them to ICANN upon request.

https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm

THE DOMAIN NAME ASSOCIATION

Healthy Domains Initiative

http://www.thedna.org/the-dna-launches-hdi-press-release-2-16-2016/

Healthy Domains Initiative Practices (February 2017)

http://thedna.org/wp-content/uploads/2017/02/DNA_Healthy_Practices_2017.pdf

NOTIFIERS

- Anti-Phishing Working Group (APWG)
  http://www.antiphishing.org/
- Center for Safe Internet Pharmacies (CSIP)
  https://safemedsonline.org/
- International Association of Internet Hotlines (INHOPE)
  http://www.inhope.org/gns/home.aspx
- Internet Watch Foundation (United Kingdom)
  http://www.antiphishing.org/
- LegitScript
  https://www.legitscript.com/
- Alliance for Safe Online Pharmacies (ASOP)
  ASOP Global: https://buysaferx.pharmacy/
  ASOP EU: http://asop.eu/

CHARACTERISTICS OF A "TRUSTED NOTIFIER" PROGRAM

Paper by Donuts in the context of its Memorandum of Understanding with the Motion Picture Association of America

http://www.donuts.domains/images/pdfs/Trusted-Notifier-Summary.pdf