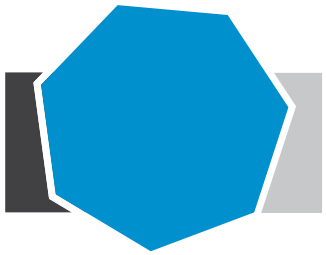


INTERNET & JURISDICTION POLICY NETWORK

DOMAINS & JURISDICTION PROGRAM

OPERATIONAL APPROACHES
NORMS, CRITERIA, MECHANISMS

APRIL 2019
www.internetjurisdiction.net

FOREWORD

When the Internet & Jurisdiction Policy Network was founded in 2012, the importance of addressing jurisdictional issues online was hardly recognized by most stakeholders. The dominant view was simply that the anticipated mass increase in internet penetration would allow people around the world to better connect and share their ideas, contribute to greater freedom and create new economic opportunities. To a large extent, many aspects of this vision have materialized in the past seven years and we now take for granted the many benefits this unprecedented collective creation of mankind has brought.

In spite of that - or maybe because of it - attention in recent years has significantly shifted: hardly a day passes without major newspapers headlines about abuses online and the difficulty to address them, given the transnational nature of the network. We may rationally recognize that such abuses remain limited in proportion of the overall online activity, but the tremendous volume of the latter legitimately make the former an increasing concern for all actors. Addressing harmful content, criminal activities and other regulatory challenges in a rights-respecting and economically sustainable manner has emerged as a crucial question for the digital 21st century.

It may have been naive to think that the dark side of human nature would not express itself also in the digital space, but it behooves all of us now to avoid letting the pendulum swing too far in the other direction. We need to find collective solutions that not only protect the precious acquis of a global network but enable our digital society to develop further in a balanced manner. This can only be achieved through cooperation similar to that which enabled the emergence of the internet itself. Unfortunately, the existing international system of separate territorial sovereignties often represents an obstacle to such cooperation.

In the absence of clear international arrangements, after a long period of inaction, the last few years have witnessed a number of separate proposals and regulations to address abuses online. However well intentioned some of them may be, unilateral decisions adopted in an uncoordinated manner under the pressure of urgency may have detrimental unintended consequences. Yet, the very proliferation of initiatives demonstrates a shared concern to address these issues. This convergence in the willingness to act must be accompanied by increased communication, coordination and cooperation between actors. It is more than ever crucial to reiterate our firm belief in the necessity to tackle common problems in a collective manner.

Given the evolution in actors' mentalities, discourse and actions that we have witnessed in the past seven years, in particular in the context of the Internet & Jurisdiction Policy Network, we should be optimistic that we can develop common frameworks benefiting all stakeholders. By working intensely and in a constructive spirit in relentless pursuit of scalable, interoperable and resilient solutions, we can together address the most pressing issues of the digital society. The following *Operational Approaches* document represents an encouraging step in this direction, concretely illustrating what can be produced when actors commit to working together in pursuit of the common public interest.

Bertrand de La Chapelle

Executive Director

Secretariat of the Internet & Jurisdiction Policy Network

TOWARDS LEGAL INTEROPERABILITY

The Internet increasingly underpins political, economic and social interactions. However, as Internet penetration grows, so do cross-border legal problems. The transnational nature of the network challenges the territorial foundation of national legal systems. The number of internet users more than doubled in the last decade, and more than half the world's population is now online. How to jointly address pressing legal challenges at the intersection of the global digital economy, human rights and security has become one of the greatest challenges of the 21st century that will define the future of the cross-border internet and the digital society.

Since 2012, stakeholders from around the world work together in the Internet & Jurisdiction Policy Network to address the tension between the cross-border nature of the Internet and national jurisdictions. Its Secretariat enables multistakeholder cooperation and facilitates a global policy process engaging over 200 key entities from more than 40 countries and all stakeholder groups: governments, the world's largest internet companies, technical operators, civil society groups, academia and international organizations.

Stakeholders in the Internet & Jurisdiction Policy Network work together in currently three thematic Programs (Data & Jurisdiction, Content & Jurisdiction and Domains & Jurisdiction) to jointly develop policy standards and operational solutions through regular virtual and physical meetings, including regional sessions and Global Conferences. The Secretariat also maintains the I&J Retrospect Database tracking global trends, and launches in 2019 the world's first Internet & Jurisdiction Global Status Report.

The regular Global Conferences of the Internet & Jurisdiction Policy Network are institutionally supported by six international organizations: Council of Europe, European Commission, ICANN, OECD, United Nations ECLAC, and UNESCO. Partners include France (2016) and Canada (2018). The work of stakeholders in the Internet & Jurisdiction Policy Network has been presented to and recognized by key international processes, including the United Nations Internet Governance Forum, G7, G20 or the Paris Peace Forum, and covered in media outlets such as The Economist, New York Times, Washington Post, Financial Times, Politico or Fortune. The work of the Policy Network is financially supported by a unique coalition of over 20 governments, companies and organizations.

FROM ISSUES FRAMING TO AREAS OF COOPERATION

After four years of international consultations and meetings in the Internet & Jurisdiction Policy Network, stakeholders gathered for the first time on a global level in Paris on November 14-16, 2016 to address the future of jurisdiction on the cross-border Internet. On this occasion, over 200 senior representatives from all stakeholder groups stressed the urgency of finding mechanisms for communication, coordination and cooperation in order to establish legal interoperability and ensure due process across borders. At this 1st Global Conference, they recognized that no actor or stakeholder group can solve these new challenges on their own: collective action was needed to prevent the escalation of a legal arms race and the proliferation of legal uncertainty. On the basis of *Framing Papers*[1] for each of the three thematic I&J Programs, they accordingly identified key *Areas for Cooperation*[2] to proceed together.

FROM POLICY OPTIONS TO THE OTTAWA ROADMAP

These *Areas for Cooperation* served as mandate for the three thematic Programs Contact Groups formed as a result of the 1st Global Conference. Composed of Members from a diverse range of entities

[1] https://www.internetjurisdiction.net/news/framing-papers-released-for-data-content-and-domains

[2] https://www.internetjurisdiction.net/uploads/pdfs/GIJC-Secretariat-Summary.pdf

and experts most engaged in the issues, they were tasked to propose what can realistically and pragmatically be achieved within each of the I&J Programs. Members, with the support of the Secretariat, mapped their respective perspectives, compared approaches, fostered policy coherence, and identified possible steps for coordinated actions. The results of these focused discussions were synthesized in *Policy Options* documents[3] released for stakeholder consultations in November 2017.

They served as official input to structure discussions at the 2nd Global Conference of the Internet & Jurisdiction Policy Network in Ottawa, on February 26-28, 2018. Over 200 stakeholders from more than 40 countries decided there on concrete focus and priorities, agreeing for the first time on Common Objectives and Structuring Questions for each of the three Programs of the Policy Network. These Work Plans were consolidated in the Ottawa Roadmap[4].

OPERATIONAL APPROACHES

Building on the methodology of the work in the I&J Programs between the 1st and 2nd Global Conferences, over 120 Members from all continents and stakeholder groups officially begun their work in August 2018 in new Contact Groups to implement the Work Plans of the Ottawa Roadmap. Three neutral Coordinators were appointed to facilitate discussions. They were respectively:

- DATA & Jurisdiction: Robert Young, Legal Counsel, Global Affairs Canada.
- CONTENT & Jurisdiction: Wolfgang Schulz, Director, Humboldt Institute for Internet and Society.
- DOMAINS & Jurisdiction: Maarten Botterman, Director, GNKS Consult.

The Members of the three Programs' Contact Groups were committed to working together and develop operational policy approaches in preparation for the 3rd Global Conference of the Internet & Jurisdiction Policy Network. The mandate for the three Programs' Contact Groups was defined on the basis of the Structuring Questions of the Ottawa Roadmap's Work Plans. Topic-specific Working Groups were established in each Program to conduct focused work and allow for more intense interactions on specific issues.

The *Operational Approaches* documents present the result of this process. They are a best effort by the Members of each Program's Contact Group to address the important cross-border issues pertaining to access to electronic evidence, content restrictions and moderation online, and requests for domain suspensions, in a manner consistent with due process and the protection of human rights.

THE 3rd GLOBAL CONFERENCE AND BEYOND

The 3rd Global Conference of the Internet & Jurisdiction Policy Network will be held on June 3-5, 2019, in Berlin, Germany. When they convene in Berlin stakeholders will discuss, on the basis of the *Operational Approaches*, how to advance the development of concrete policy standards and operational solutions. The *Berlin Roadmap* that will come out of this 3rd Global Conference will guide the next phase of work of stakeholders in the Programs of the Internet & Jurisdiction Policy Network, in particular:

- How proposals in the *Operational Approaches* documents (Norms, Criteria and Mechanisms) can be used to enhance legal interoperability;
- How to structure further work on issues already identified that require or warrant more in-depth discussions;
- How to address new issues identified at the 3rd Global Conference in a solutions-oriented manner.

[3] *https://www.internetjurisdiction.net/news/policy-options-documents-released-for-the-2nd-global-internet-and-jurisdiction-conference*

[4] *https://www.internetjurisdiction.net/news/outcomes-of-the-2nd-global-conference-of-the-internet-jurisdiction-policy-network*

CONTEXT

ADDRESSING ABUSE AT THE DNS LEVEL - THE CHALLENGE

The internet addressing system is essential for the proper functioning of the global network that now underpins most human activities. Domain names ensure a user-friendly conversion between human-readable identification strings and the long numerical Internet Protocol (IP) addresses indicating the location of a particular server on the network. The Domain Name System (DNS) is managed[1] by a distributed set of technical operators, mainly: Registries in charge of Top Level Domains (ccTLDs and gTLDs[2]), and Registrars distributing domains at the second level to Registrants. The Internet Corporation for Assigned Names and Numbers (ICANN) has the mission[3] to "ensure the stable and secure operation of the internet's unique identifier systems" and in particular to "coordinate the development and implementation of policies concerning the registration of second-level domain names in generic top-level domains ("gTLDs")".

Preserving the neutrality of the technical layer is important to ensure trust in the DNS. When dealing with potential abuses, there is a traditional distinction[4] between registration abuse and use abuse. The former is "related to the core domain name-related activities performed by registrars and registries," whereas the latter "concerns what a registrant does with his or her domain name after the domain is created - the purpose the registrant puts the domain to, and/or the services that the registrant operates on it." While the former is fully within ICANN's remit, its Bylaws indicate that "ICANN shall not regulate (i.e., impose rules and restrictions on) services that use the Internet's unique identifiers or the content that such services carry or provide".

Yet, pressure is mounting to leverage domain names to address illegal activities or content on underlying websites. Use abuse covers two dimensions: technical abuse (e.g. phishing, malware distribution, etc.), which is closely related to the security and stability of the DNS, and abusive content (e.g. child abuse material, intellectual property violations, etc.). Registries and Registrars (DNS Operators) are very diverse in terms of size, activities or governance structures. Moreover, the fundamental distinction between country code and generic TLDs in terms of relation with national laws and authorities, leads to very different approaches and constraints when receiving direct requests or orders for action at the DNS level regarding use abuse, particularly when they originate across borders. In the absence of a generally accepted framework regarding how to deal with use abuse, DNS Operators' practices vary considerably.

This situation raises two fundamental questions: 1) when can it be appropriate to act at the DNS level to address abuses? and 2) who should have the responsibility of making this decision?

APPROPRIATENESS OF ACTION AT THE DNS LEVEL

On a principle level, given the neutral function of the DNS and the overarching norm of proportionality, the fact that a domain suspension has a global impact by nature calls for a high threshold of abusive activity or content to justify such a measure. A fundamental criterion to take into account is also the

---

[1] *A more detailed explanation of this architecture can be found here: https://whois.icann.org/en/domain-name-registration-process*

[2] *Country-code Top Level Domains (ccTLDs) are two-letter extensions, such as .uk, .br or .fr, corresponding to countries, according to an ISO list; Generic Top Level Domains (gTLDs) include the original .com, .net, .org and now more than a thousand new ones introduced more recently. For more on this important distinction, see: https://websapiens.eu/site/artile.php?aid=31&cid=26*

[3] *See: https://www.icann.org/resources/pages/governance/bylaws-en/#article1*

[4] *See the report from ICANN's gNSO Registration Abuse Policies Working Group: https://gnso.icann.org/sites/default/files/filefield_12530/rap-wg-final-report-29may10-en.pdf*

actual involvement and intent of the registrant in the infringing behavior or content. Finally, irrespective of harm types, blocking at the DNS level is a blunt tool that does not allow limiting access to specific pieces of content. It can even have a limited efficiency in preventing users from getting access to the resource they want to reach (e.g. directly through the IP address). Other actors, such as hosting providers, are also often more able to provide a proportionate response.

In light of the above, DNS Operators are more inclined to take action at the level of the DNS in response to technical abuse than when dealing with abusive content that they usually do not have the competence to properly evaluate given the diversity of applicable national laws, unless a clear threshold of abuse is met.

DECISION-MAKING

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

In that respect, court orders can provide procedural guarantees and clarity of applicable law. DNS 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, national court decisions regarding a domain name can mean imposing the legislation of one particular country over registrants, activities and users around the world something that can confer strong power to countries where many operators are located.

In this context, self-established specialized "notifiers" of various sorts and structures document perceived abuses and propose formal agreements to DNS Operators. However, no external "accreditation" mechanism exists to certify their credibility and they currently only have the authority that Operators accept to bestow upon them. DNS 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.

COOPERATION FRAMEWORK

The different actors recognize the difficulty of addressing these issues. They expressed interest in working together to define under which strict conditions acting at the DNS level may be appropriate to address use abuse, as well as rules and procedural guarantees that could help establish the credibility of specialized notifiers.

The work of the dedicated Contact Group of the Internet & Jurisdiction Policy Network, as presented in this Operational Approaches document, aims to contribute to this discussion by addressing the key elements of a voluntary framework on the mutual responsibilities of the different actors regarding actions at the DNS level.

The Internet & Jurisdiction Secretariat

TABLE OF CONTENTS

COORDINATOR'S MESSAGE

The internet was never built for all that it is used for today. It has grown to become a network of networks that facilitates economic, social, and scientific interaction around the world, across borders and virtually independently from vast distances. This rapid expansion challenges us to adapt the way we work, interact, and organize ourselves and our societies.

The Internet & Jurisdiction Policy Network addresses one of the "unintended consequences" of the Internet: how to deal with interactions across jurisdictions, including potential harmful or criminal activities across borders. It is in the interest of all legitimate parties to keep the internet not only secure and stable, but also safe and reliable for all its users. A balance must be found between allowing people to use the internet freely, and recognizing and addressing abuse in a proportionate, yet effective way.

This goes beyond the mission of one stakeholder or group of stakeholders alone. What role Domain Name System (DNS) Operators can and cannot reasonably play in that regard is of particular importance.

In Paris, in 2016, the 1st Global Conference of the Internet & Jurisdiction Policy Network initiated a structured process, reinforced after the 2nd Global Conference, held in Ottawa, in February 2018. Many fruitful debates were conducted in dedicated Contact Groups through virtual and physical meetings around the world. These discussions led to the present *Operational Approaches* document. Informed by real practice experience, it provides real insight on what would make sense to do, today, on a voluntary basis, to address different types of abuses.

Over these years, all stakeholders participated on an equal footing, and generously contributed their time and experience, in full respect for each other's opinions and perspectives. It has been a pleasure and an honor to work with the Internet & Jurisdiction Secretariat as well as the Members of the Contact Group on what I believe is a useful contribution to our understanding of what we can do together: legal, scalable, and reasonable solutions for both users and service providers.

I think it is fair to say we all learned from each other, and we managed to take a step forward. By no means are the issues all solved. However, this step, and more steps like this one, will help the internet – which is not good or bad in itself – to be used in a way that is most effective, and safe for us all.

Maarten Botterman,

Coordinator,

Domains & Jurisdiction Program's Contact Group

MEMBERS OF THE DOMAINS & JURISDICTION PROGRAM'S CONTACT GROUP

The Secretariat appointed a neutral Coordinator to facilitate the work of the Contact Group:

- **MAARTEN BOTTERMAN**, Director, GNKS Consult and Board Director, ICANN

The discussions in Working Groups, which helped conduct focused work on specific topics, were moderated by neutral Facilitators:

- **SUSAN CHALMERS**, Internet Policy Specialist, United States, Department of Commerce NTIA
- **BRIAN CIMBOLIC**, Vice President and General Counsel, Public Interest Registry

MEMBERS OF THE CONTACT GROUP

BENEDICT ADDIS	Chair, Registrar of Last Resort (RoLR)
FIONA ALEXANDER	Associate Administrator, United States, Department of Commerce NTIA
TIJANI BEN JEMAA	Executive Director, Mediterranean Federation of Internet Associations
JAMES BLADEL	Vice President of Policy, GoDaddy
MAARTEN BOTTERMAN	Board Director, ICANN
JORDAN CARTER	Chief Executive, InternetNZ
MISHI CHOUDHARY	Legal Director, Software Freedom Law Centre
BRIAN CIMBOLIC	Vice President and General Counsel, Public Interest Registry
KEITH DRAZEK	Vice President, Public Policy and Government Relations, VeriSign
HEATHER DRYDEN	Senior Advisor, Canada, Department of Innovation, Science and Economic Development
RITA FORSI	Director General, Superior Institute for Communications and Information Technology, Italy, Ministry of Economic Development
JOTHAN FRAKES	Executive Director, Domain Name Association (DNA)
DEMI GETSCHKO	CEO, Network Information Center for .BR
GRACE GITHAIGA	Co-convener, Kenya ICT Action Network (KICTANET)
HARTMUT GLASER	Executive Secretary, Brazilian Internet Steering Committee (CGI.br)
RAHUL GOSAIN	Director, IRSME, India, Ministry of Electronics and Information Technology
RUDOLF GRIDL	Head of Division, Internet Governance, Germany, Federal Ministry for Economic Affairs and Energy
ROB HALL	CEO, Momentous
STATTON HAMMOCK	Vice President of Global Policy and Industry Development, MarkMonitor
BYRON HOLLAND	President and CEO, Canadian Internet Registry Authority (CIRA)
WILL HUDSON	Senior Advisor for International Policy, Google

MANAL ISMAIL	Executive Director, International Technical Coordination, Egypt, National Telecommunications Regulatory Authority
KONSTANTINOS KOMAITIS	Senior Director, Strategy and Policy Development, Internet Society
MARILIA MACIEL	Digital Policy Senior Researcher, Diplo Foundation
DESIREE MILOSHEVIC	Senior Advisor, International Affairs and Public Policy, Afilias
PAUL MITCHELL	Senior Director, Technology Policy, Microsoft
CRISTINA MONTI	Policy Officer, International Data Flows and Protection, European Commission, DG JUST
MICHELE NEYLON	CEO, Blacknight Internet Solutions
SEUN OJEDEJI	Chief Network Engineer, Federal University of Oye-Ekiti
CRYSTAL ONDO	Vice President, Corporate Affairs, Donuts
ROD RASMUSSEN	Principal, R2 Cyber
BRYAN SCHILLING	Consumer Safeguards Director, ICANN
JORG SCHWEIGER	CEO, DENIC
GEO VAN LANGENHOVE	Legal Manager & Data Protection Officer, European Registry of Internet Domain Names (EURid)
PETER VAN ROSTE	General Manager, Council of European National Top-Level Domain Registries (CENTR)
CHRIS WILSON	Senior Manager, Public Policy (Internet Governance), Amazon Web Services

In addition to the Members of the Contact Group, the Secretariat wishes to thank the following actors for their engagement in discussions held in the Contact Group and its Working Groups.

MOHIT BATRA	Technology Analyst, National Internet Exchange of India (NIXI)
ELIZABETH BEHSUDI	Former Vice President and General Counsel, Public Interest Registry
DIEGO CANABARRO	Expert Advisor to the Board, Brazilian Internet Steering Committee (CGI.br)
BRENT CAREY	Domain Name Commissioner, New Zealand Domain Name Commission
SUSAN CHALMERS	Internet Policy Specialist, United States, Department of Commerce NTIA
GUNTHER GRATHWOHL	Counsellor, Germany, Federal Ministry for Economic Affairs and Energy
ALLAN MACGILLIVRAY	Senior Policy Advisor to the President, Canadian Internet Registration Authority (CIRA)
POLINA MALAJA	Policy Advisor, Council of European National Top-Level Domain Registries (CENTR)
JULIE MICHEL	Legal Counsel, European Registry of Internet Domain Names (EURid)
DAVID PAYNE	Vice President, Compliance, Afilias
MATHIEU POTTER	Policy Analyst, Canada, Department of Innovation, Science and Economic Development
VINICIUS SANTOS	Technical Advisor, Brazilian Internet Steering Committee (CGI.br)

SYNTHESIS OF THE OPERATIONAL APPROACHES

The following *Operational Approaches* document is the result of a best effort by the Members of the Domains & Jurisdiction Program's Contact Group to address the important issues identified in the *Ottawa Roadmap* of the 2nd Global Conference of the Internet & Jurisdiction Policy Network on February 26-28, 2018. The Work Plan that was refined there identified 11 important Structuring Questions to further guide interactions within the Domains & Jurisdiction Program. The present *Operational Approaches* are a joint contribution by some of the most engaged experts in this field to the ongoing debate on the complex issues of when and how it may be appropriate to take action at the DNS level to address abuses. **They should however not be understood as the result of a formal negotiation validated by these Members' organizations.**

On this basis, the Members of the Program's Contact Group, with the help of the Secretariat, produced the attached set of proposed Operational Norms, Criteria and Mechanism to provide a common frame of reference for the various actors when implementing or developing voluntary practices to address abuses. These *Operational Approaches* intend to help educate the general public about the conditions under which it may be appropriate to act at the DNS level to address both technical and website content abuses in full respect of international human rights principles. This document can also help public and private decision-makers take into account the full range of relevant parameters when developing and implementing responsible frameworks, rules and practices in that regard.

Taking into account the limited time available to address these complex issues, the work of the Members of the Program's Contact Group was distributed among four thematic Working Groups, to propose, draft and refine elements that are documented according to the three-part structure presented on page 16.

These *Operational Approaches* will feed into the 3rd Global Conference of the Internet & Jurisdiction Policy Network on June 3-5, 2019 in Berlin, which is organized in partnership with the Government of the Federal Republic of Germany, and institutionally supported by the Council of Europe, European Commission, ICANN, OECD, United Nations ECLAC, and UNESCO.

STRUCTURE OF THE OPERATIONAL APPROACHES

The *Operational Approaches* document is organized according to the following three-part structure.

OPERATIONAL NORMS

This section identifies a set of norms that can help organize actors' behavior in their own actions and their mutual interactions. They focus on the operational level within the context of existing high-level principles.

The Domains & Jurisdiction Operational Norms specifically identify elements pertaining to the appropriateness of acting at the DNS level, notification mechanisms for Registries and Registrars (DNS Operators), appropriate action, and procedural guarantees.

OPERATIONAL CRITERIA

This section contains lists of elements or criteria that can be used by all categories of decision-makers when developing, evaluating, and implementing solutions. The purpose is for all actors to be able to discuss ideas, evaluate initiatives and debate proposals using common frames of reference and structuring questions.

The Domains & Jurisdiction Operational Criteria address four important themes in the debate related to the appropriateness of acting at the DNS level: **(I) Level of Action**, including the types of abuses for which it may be appropriate to act at the DNS level and the corresponding thresholds; **(II) Proper Notices**, including the components of a complete request, notifier types and expected due diligence by Notifiers; **(III) Requested Actions**, including the possible action types that are at the disposal/applicable at the level of the DNS Operators; and **(IV) Procedural Guarantees**, including transparency, guiding criteria regarding notification of registrants and recourse modalities if they want to contest complaints or actions against their domain names.

OPERATIONAL MECHANISM

This third section presents a proposal for which operationalization efforts can be initiated in the period following the 3rd Global Conference of the Internet & Jurisdiction Policy Network, in Berlin.

The concept note explores how an easy to use abuse reporting interface could be envisaged to send properly documented notices to the right recipients, and how to best organize the next steps during the 3rd Global Conference and in the follow-up work.

OPERATIONAL NORMS

Any voluntary approach regarding requests for action at the DNS level to address technical abuse and abusive content must duly address:

LEVEL OF ACTION

Thresholds - Clear and high threshold criteria determine when taking action at the DNS level may be appropriate to address technical abuse and abusive content.

Terms of Service (ToS) - DNS Operators' ToS clearly describe the types of abuses they are willing to address and the applicable procedures to report it.

PROPER NOTICES

Recipients - When action at the DNS level is justified, Registrars should be the first recipients of abuse notices, as their direct relation to the registrant enables effective action.

Point(s) of Contact - Each DNS Operator indicates in a transparent manner and publicly advertises the Abuse Point(s) of Contact to which notices should be addressed.

Formats - Shared components for notices facilitate evaluation of their completeness, quality and relevance, thus helping structure interactions between notifiers and DNS Operators.

Substance - Individual notices provide sufficient supporting information and proof of prior due diligence to appreciate if the level of alleged abuse justifies the requested action.

ACTIONS

Technical feasibility - Requested actions must be technically implementable by DNS Operators, and sufficient information is provided in notices for their execution if deemed justified.

Appropriate action - Among all possible measures, the action implemented is the most reasonable, in accordance with the standards of necessity and proportionality, and taking into account potential collateral impact.

Reversibility - Actions implemented are as reversible as possible, to allow for restoration of the DNS service if appropriate.

PROCEDURAL GUARANTEES

Due diligence - Prior to alleging that a domain name is associated with abuse, notifiers will conduct substantive and procedural due diligence. Upon reception of notice, DNS Operators will conduct similar due diligence as part of their investigation.

Notifier Agreement - Any contractual agreement between a DNS Operator and a specialized notifier defines their respective responsibilities and establishes clear criteria to ensure due process.

Responses - DNS Operators acknowledge receipt of notices, and, when issued by public authorities, inform them whether actions were taken.

Notification - Registrants are notified of alleged abuse before a Registrar or Registry acts against a domain name. For some allegations of abuse where this is not practical, advisable, or even permissible, notification is promptly provided after the fact, unless legally prohibited.

Recourse - DNS Operators and notifiers maintain a publicly identifiable process allowing registrants to contest or appeal an action against a domain name following a notice of abuse, by providing independently verifiable evidence that does not require (or at least minimizes the need for) the DNS Operator to interpret the law.

OPERATIONAL CRITERIA

The following criteria represent the best efforts by the members of the Domains & Jurisdiction Program's Contact Group and its Working Groups, as compiled by the I&J Secretariat, in identifying concise lists of elements that can be used by all categories of decision-makers when developing, evaluating, and implementing solutions. The purpose is for all actors to be able to discuss ideas, evaluate initiatives and debate proposals using common frames of reference and structuring questions.

The following documents should be understood as basis for future reference and work in the Internet & Jurisdiction Policy Network, following its 3rd Global Conference. Below is the list of Operational Criteria for the Domains & Jurisdiction Program:

PART I - LEVEL OF ACTION

- CRITERIA A - Types of Abuses
- CRITERIA B - Thresholds

PART II - PROPER NOTICES

- CRITERIA C - Notice Components
- CRITERIA D - Notifier Types
- CRITERIA E - Due Diligence by Notifiers

PART III - ACTIONS

- CRITERIA F - Types of Actions

PART IV - PROCEDURAL GUARANTEES

- CRITERIA G - Transparency
- CRITERIA H - Notification to Registrants
- CRITERIA I - Recourse for Registrants

PART I - LEVEL OF ACTION

CRITERIA A - TYPES OF ABUSES

DNS Operators receive cross-border requests to take action against domain names allegedly associated with technical abuse or problematic content. Listed below are descriptions of different types of technical abuses, as well as website content abuse, for which Registries and Registrars often receive such requests.[1]

1. **Technical abuses**
   Domain names can be misused to propagate different types of technical abuse, including but not limited to the following:

   a. **Spam** is unsolicited bulk email, where the recipient has not granted permission for the message to be sent, and where the message was sent as part of a larger collection of messages, all having substantively identical content.[2] Spam email may carry malware, and/or deliver phishing or pharming attacks.

   b. **Malware** is malicious software, installed on a device without the user's consent, which disrupts the device's operations, gathers sensitive information, and/or gains access to private computer systems. Malware includes viruses, spyware, ransomware, and other unwanted software.[3]

   c. **Phishing** occurs when an attacker tricks a victim into revealing sensitive personal, corporate, or financial information (e.g. account numbers, login IDs, passwords), whether through sending fraudulent or "look-alike" emails, or luring end users to copycat websites. Some phishing campaigns aim to persuade the user to install software, which is in fact malware.

   d. **Pharming** is the redirection of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning. DNS hijacking occurs when attackers use malware to redirect victims to their own site instead of the one initially requested. DNS poisoning causes a DNS server to respond with a false IP address bearing malicious code.[4] Phishing differs from pharming in that the latter involves modifying DNS entries, while the former tricks users into entering personal information.

   e. **Botnets** are collections of Internet-connected computers that have been infected with malware and commanded to perform activities under the control of a remote administrator.[5]

   f. **Fast-flux hosting** is used to disguise the location of Web sites or other Internet services, or to avoid detection and mitigation efforts, or to host illegal activities. Fast-flux techniques use

---

[1] *These lists are illustrative and not intended to be exhaustive.*

[2] *See "The Definition of Spam" by The Spamhaus Project, at https://www.spamhaus.org/consumer/definition/*

[3] *See M3AAWG & London Action Plan, Operation Safety-Net: best practices to Address Online Mobile and Telephony Threats (2015) ("Operation Safety-Net"), at https://www.m3aawg.org/system/files/M3AAWG_LAP-79652_IC_Operation_Safety-Net_Brochure-web2-2015-06.pdf; "Malware" page at the U.S. Federal Trade Commission website, at https://www.consumer.ftc.gov/articles/0011-malware*

[4] *See the Public Interest Registry's Domain Name Anti-Abuse Policy, at https://pir.org/policies/org-idn-policies/anti-abuse-policy/; entries for DNS hijacking and DNS poisoning in the Kaspersky Lab Encyclopedia, at https://encyclopedia.kaspersky.com/glossary/dns-hijacking/*

[5] *See "A Glossary of Common Cybersecurity Terminology," National Initiative for Cybersecurity Careers and Studies, at: https://niccs.us-cert.gov/about-niccs/glossary#B*

the DNS to frequently change the location on the Internet to which the domain name of an Internet host or name server resolves.[6]

2. **Website content abuses**

Most DNS Operators treat requests to deal with problematic website content differently from technical abuses. Since Registries and Registrars (when not also serving as the hosting provider) cannot remove offending pieces of content from a website, more often than not, acting at the DNS level is not appropriate. Remediation for problematic content should occur at the registrant or hosting provider level.

The descriptions below are derived from various sources, including input from Contact Group members. They are neither offered nor intended to be interpreted as normative descriptions. Some types of problematic content find a higher degree of shared agreement across jurisdictions than others.

a. **Child abuse material** consists of photos or videos taken by an offender, documenting the sexual abuse of a child.[7]

b. **Controlled substances and Regulated goods** for sale or trade include illegal drugs, the illegal sale of legal drugs, illegal services, stolen goods, and illegal firearms or other weapons. The legality of a given substance or good will vary across jurisdictions.

c. **Violent extremist content** includes content that depicts graphic violence, encourages violent action, endorses a terrorist organization or its acts, or encourages people to join such groups.

d. **Hate speech** includes advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.[8]

e. **Intellectual property** related domain name suspension requests in response to website content (not relating to the domain name itself) have been issued on the basis of alleged trademark (e.g. sale of counterfeit goods), patent or trade secret infringement, or piracy of copyrighted works. As with all categories above, laws regarding intellectual property differ across jurisdictions.

---

[6] *See the Public Interest Registry's Domain Name Anti-Abuse Policy, at https://pir.org/policies/org-idn-policies/anti-abuse-policy/*

[7] *Interpol, "Online child abuse material: Q & A" (January 2017). https://www.interpol.int/Media/Files/Crime-areas/Crimes-against-children/Online-Child-Abuse-%E2%80%93-Questions-and-Answers/*

[8] *International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR), Art. 20(2), at https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx*

---

[1] *See Content & Jurisdiction Operational Approaches document, Operational Criteria B - Normative Basis*

CRITERIA B - THRESHOLDS

1. **Technical abuse**
   Acting at the DNS level is generally justified in situations of technical abuse in order to protect the stability and security of the global infrastructure of the internet. Specific additional measures are nonetheless justified to assist the registrant if the domain is obviously compromised by third parties without his/her knowledge.

2. **Abusive content**
   On the other hand, given the geographically global impact of an action at the DNS level, doing so regarding abusive content can only be justified if a particularly high threshold of abuse/harm is met, regarding inter alia:

   a. The degree of global normative consistency[1] regarding the alleged abuse: i.e. whether the content at issue is considered illegal across a sufficient number of jurisdictions;

   b. The proportion of the site effectively dedicated to the infringing content;

   c. The manifest intended purpose or bad faith of the registrant, and

   d. The lack of available alternative measures to remediate the situation.

PART II - PROPER NOTICES

CRITERIA C - NOTICE COMPONENTS

DNS Operators frequently receive notices of abuse in a broad diversity of formats that often do not contain sufficient information for investigation and action. The following table therefore proposes a list of components that good notices should contain to facilitate interactions between issuers and DNS Operators.

IDENTIFICATION	
Request ID number	Reference provided by the issuer of the request.
Time	Date or more precise timestamp corresponding to the issuance of the request.
Issuing Entity	Nature and precise identification of the requester: court, law enforcement, notifier, legal representative of a complainant.
Requested Registrar	Name and abuse POC of the Registrar managing the registration.
Relevant Registry	Registry managing the corresponding TLD extension (for information).
CASE	
Type of abuse	Security and stability abuse or abusive content (from taxonomy list).
Supporting evidence	Factual documentation of the alleged abuse.
Proportionality	Justification that the alleged abuse meets the required threshold for action.
Legal basis	Court decision or applicable law if notice by public authority.
DUE DILIGENCE	
Evaluation	Steps undertaken by the private notifier - prior to notification of the DNS Operator - to ascertain the reality and extent of the abuse, in relation to pre-agreed standards and applicable law(s).
Prior measures	Steps taken by the private notifier - prior to notification of the DNS Operator - to contact the registrant and request cessation of the abuse (when applicable).
REQUESTED ACTION	
Targeted domain(s)	Specific domain name(s) upon which action is requested, identified through the specific URL(s) where abuse is alleged.
Action sought	Indication of the specific action requested (see Criteria F - Types of Actions) and provision of relevant information to technically execute it.
TIMING	
Deadline	When the actions should be executed (important in particular in case of concerted actions or emergency).
Time range	Duration of the requested action (if applicable).
Emergency	Is this action justified by a particular emergency (nature of emergency).
Rationale emergency	Clarification of link of requested action to emergency and how it will avert the emergency.

CONFIDENTIALITY	
Confidentiality	Request not to notify the registrant prior to action or potentially even ex post for a period of time (if applicable).
Rationale for confidentiality	Proper justification for such confidentiality.
Confidentiality timeline	Time limit for absence of notification.
AUTHORITY	
Authentication	Information allowing verification of the identity of the public authority requester and the authenticity of its notice.
Certification	Written self-certification by the private notifier of its authority, performance of prior due diligence and accuracy of its statements.
CONTACTS	
Issuing entity	Contact details of the requesting entity, to which notification of action (or non-action) should be sent.
SIGNATURE	

CRITERIA D - NOTIFIER TYPES

1. **Orders from the DNS Operator's jurisdiction**
   DNS Operators can be lawfully required to comply with court orders from their jurisdiction (including foreign orders that have been "domesticated"). Competent authorities should however responsibly exercise this authority to avoid disproportionately imposing their national laws on content produced and hosted legally in other parts of the world (see Operational Criteria B - Thresholds).

2. **Other sources of notices**
   a. Courts outside the jurisdiction where the DNS Operator is incorporated may issue cross-border notices for action at the DNS level. Although they are not directly enforceable per se, DNS Operators may, within the framework of their Terms of Service, take action as a result in light of the procedures followed locally and their own investigation of the facts available to them.

   b. Specialized notifiers representing public or specific interests issue notices to DNS Operators. The latter determine after investigation whether to take action or not, based on the demonstration of the requisite level of due process and due diligence followed, and their pre-existing relationship with the notifier (contractual or otherwise).

   c. Concerned individuals send notices through DNS Operators' abuse points of contact to bring to their attention abuses they believe should be acted upon at the DNS level.

CRITERIA E - DUE DILIGENCE BY NOTIFIERS

1. **General principle**

   Persons or entities that file complaints or make abuse notices (notifiers) to domain name Registrars and Registries should ensure that they have conducted proper due diligence (both substantive and procedural) prior to alleging a domain name is engaged in abuse, either DNS/technical abuse (security and stability abuses) or in the context of content complaints (website content abuses).

2. **Operational considerations**

   a. **Substantive due diligence**

   Substantive due diligence involves ensuring that any claim against the content of any domain is properly investigated, substantiated and documented (e.g., screen shots, listing on any blacklists, evidence of ownership in claims of infringement). A notifier should ensure that it has undertaken proper substantive due diligence before making a referral.

   b. **Procedural due diligence**

   Procedural due diligence involves a hierarchy (see Table 1 below) of where the notice should be made.

   For technical abuse, notices directly to the Registrar and Registry are appropriate. In instances of content complaints, mitigation at the DNS level is an imperfect remedy. Accordingly, notices should be made in the following order:

Table 1 - Proper content complaint referral paths

Currently, some notifiers for content complaints make their referrals directly to the Registry or Registrar. This can lead to problems with proportionality.

i. Using the example of a file sharing site, if a Registrar or Registry suspends the entire domain because of an allegation regarding a limited number of infringing or offensive content, then potentially thousands of other pieces of legitimate content are rendered inaccessible by not just the registrant, but end users.

ii. The website operator, registrant or hosting provider, however, can all affect and likely remove the limited instances of abusive content while leaving the remaining content (as well as the domain name) unaffected.

Accordingly, for content complaints, a notifier should first attempt to work with the website operator, the registrant and the hosting provider to have the specific pieces of content removed. If none of those actors ultimately act or remove the content, the notifier may wish to escalate to the Registrar or Registry (such referral would still be subject to applicability of any Acceptable Use or similar policy).

PART III - ACTIONS

CRITERIA F - TYPES OF ACTIONS

Protection of the core of the Internet is and should be a key priority. The DNS - part of the core of the internet - is an addressing system. It is a neutral, technical layer that is vital for the proper functioning of the Internet. Action at the DNS layer is neither a fully effective way - nor should be considered as the natural tool - to address technical abuses or problematic content.

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 the suspension of a domain has by definition a global impact, proportionality requires 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.

Requests for domain name suspension should be directed in the first instance to those parties that are closest to the abusive activity, including by contractual relationship (see Table 1 in Criteria E - Due Diligence by Notifiers for more detail). For example, requestors should first attempt to contact the domain name registrant, and then the hosting provider (either or both of which may be the wrongdoer), as these parties have the most direct relationship to the website content.[1] Direct action by registrants or hosting providers_minimizes potential impact on the functioning of DNS. If these attempts are unsuccessful, requestors should consider the below options. Listed below are different types of actions that Registry operators and Registrars may take, as appropriate, in response to cross-border suspension requests.[2]

Note that the availability of any given action below may vary across providers.

1. For Registries: **Refer the suspension request to the Registrar**, which has the contractual relationship with the Registrant of the domain name.
2. **Hold** the domain name so it does not resolve. This removes the domain name from the TLD zone file, so the domain name will no longer resolve on the public Internet. In the event that the request was made in error, this action may be reversed.
3. **Lock** the domain name so it cannot be changed. A locked domain cannot be transferred, deleted or have its details modified, but will still resolve.
4. **Redirect** name services for the domain name. A Registry has the technical ability to change a domain name's nameservers. By changing the nameservers for the domain name, services associated with the domain name can be redirected for "sink-holing" (logging traffic) to identify victims for the purposes of remediation.
5. **Transfer** the domain name to a suitably-qualified Registrar may prevent exploitation, whilst allowing for management of lifecycle, EPP status codes, and expiration.
6. **Delete** the domain name. Deletion is an extreme action and not generally recommended without careful due diligence and direction from the appropriate authorities. Restoring a domain name, if the deletion is found to be inappropriate, may involve additional burdens that are not manifest when placing a domain name on hold. Deletion is generally not as effective at mitigating abuses as suspension, as a registrant is free to re-register the domain name after it is purged from the zone.

---

[1] *See CENTR, Domain name registries and online content (Jan 30, 2019), available at: https://centr.org/library/library/centr-document/domain-name-registries-and-online-content.html (describing the relationships between various actors involved with a website featuring abusive content).*

[2] *These actions are adapted from ICANN's Framework for Registry Operator to Respond to Security Threats, at, https://www.icann.org/resources/pages/framework-registry-operator-respond-security-threats-2017-10-20-en. (Internal citations omitted).*

PART IV - PROCEDURAL GUARANTEES

CRITERIA G - TRANSPARENCY

A two-dimensional approach can help to improve transparency:

1. **Statistics**
   Beyond metrics currently used for performance measurement, DNS Operators would be encouraged to develop metrics for collecting and reporting, in exportable, and accessible formats, coherent statistics pertaining to abuse notifications and implemented actions. Public authorities and specialized notifiers should likewise develop corresponding mechanisms to ensure traceability of their notices.

2. **Decision-making**
   DNS Operators document and make available to the public the criteria determining when action at the DNS level is appropriate, the types of abusive content they are willing to take action on, and their abuse point(s) of contact. They also document and publicize their internal criteria for decision-making and the channels for appeals/recourse. Specialized notifiers likewise document and make available to the public their criteria for evaluation of abuses, as well as their due diligence rules and procedural guarantees.

CRITERIA H - NOTIFICATION TO REGISTRANTS

1. **General principle**
   Registrants should generally be provided with notifications of alleged abuse before a Registrar or Registry acts against a domain name. There are, however, some allegations of abuse where this is not practical, advisable, or even permissible, and in those instances, notification after the fact should be provided, unless legally forbidden.

2. **Operational considerations**
   a. **Registrant notification before action**
      If a Registry or Registrar receives allegations of copyright infringement, allegations of defamation, instances where content may be inferred to be illegal or fraudulent but cannot be proven without further investigation[1] (generally, "content complaints"), notification to the registrant should occur prior to a DNS Operator taking action on the domain.

   b. **Registrant notification after action**
      If a Registry or Registrar receives allegations of DNS technical abuse ("technical abuse"), court orders from competent jurisdiction(s) directing action or as set forth in applicable Registrar or Registry policies or procedures, notification to the registrant can occur after the fact.[2]

   c. **Who provides the notification?**
      Between the Registrar and Registry, Registrars are the preferred operator to provide

[1] This assumes the various categories of content fall within the scope of the Registry or Registrar's Terms of Service, Anti-Abuse or Acceptable Use Policies or other governing terms. If the content falls outside the scope of such terms, no Notification will be typically provided and the domain will not be actioned.

[2] There are also instances when a DNS Operator cannot provide Notification at all (such as when a court order requires confidential handling, or after weighing relevant law enforcement considerations).

notifications to registrants. Registrars usually have a closer contractual and business relationship with the registrant, and the Registrar collects the registrant's information. Many ccTLD Registries have direct contractual or business relationships with the registrant and may be similarly positioned to provide notifications.

gTLD Registries typically (but not always) provide notifications to Registrars who are asked to work with the registrant to remediate the alleged abuse. In non-court-mandated situations, abuse notifications are usually sent to the Registrar who is then requested to work with the registrant in a limited time frame (e.g. 48 hours) to remediate the alleged abuse.

d. Content of the notice

In most cases, only information necessary to inform the registrant's investigation and remediation of the alleged abuse should be provided in a notification. In some instances, the entire referral may be transmitted (e.g., in instances of alleged copyright infringement if that is in scope of the relevant parties' terms).

CRITERIA I - RECOURSE FOR REGISTRANTS

1. General principles

Registrars and Registries should maintain a publicly available process (even an informal one) for allowing a registrant to contest or appeal an action against a domain name for technical abuse or for a content complaint. Any appeal must include independently verifiable evidence that does not require (or at least minimizes the need for) the DNS Operator to interpret the law, which is generally outside the DNS Operator's expertise.

2. Operational considerations

a. Process

Registries and Registrars should note in their Anti-Abuse Policy/Acceptable Use Policy how such an appeal can be lodged.

i. This will typically be something along the lines of "For inquiries regarding actions taken pursuant to this policy, please contact [abuse@example.example or review@example.example]"

This process will be available for actions except those carried out pursuant to a court order from the DNS Operator's jurisdiction. If action was taken pursuant to an order from a court with jurisdiction over the DNS Operator, no internal DNS Operator process can overrule such an order.

The DNS Operator should conduct proper and thorough due diligence before action on the domain is effectuated. This should obviate the need for much back-and-forth with the registrant on appeal.

b. Evidence submitted

Registries and Registrars are not courts of competent jurisdiction, nor are they experts in interpreting various applicable laws. Accordingly, any evidence submitted by a registrant/appellant must be independently verifiable and not require (or at least minimize the necessity for) the DNS Operator to interpret the law. For a DNS Operator to reverse its decision in such an appeal, the evidence must be overwhelming and objective. It is important to have such a mechanism in case for instance of DNS Operator error or overwhelming evidence provided against the notifier's complaint.

c. Overturning action regarding technical abuse

There is less "wiggle room" in evaluating technical abuse than in evaluating abusive content. If a domain was engaged in phishing or distribution of malware and identified as such, only evidence clearing a high threshold should allow for reversal of a suspension, unless the domain has been compromised.

i. If a registrant is able to show the domain was compromised without his/her knowledge, the DNS Operator may wish to consider such evidence.

ii. Another instance for a DNS Operator to reverse a decision for technical abuse would be for DNS Operator error, such as suspending the wrong domain name (example1.example instead of example11.example), or if a domain was removed from a blocklist that was relied upon prior to suspension.

d. Overturning action regarding website content abuse

There is more room for interpretation here by a DNS Operator for content complaints, but any evidence submitted must be independently verifiable and not require, or at least minimize the necessity for, the DNS Operator to interpret the law.

If a registrant appeals action a DNS Operator took due to reliance or work with a third party (such as a specialized notifier), the DNS Operator and notifier should have a process in place whereby the notifier can independently assess the countervailing evidence and be willing to reverse its recommendation.

OPERATIONAL MECHANISM

INTERFACE FOR ABUSE REPORTING TO DNS OPERATORS

CONTEXT

All actors have a common interest that actual abusive content can be reported to the right DNS Operator with sufficient justifying information to enable decision and proportionate action when it is justified to act at the DNS level. Two challenges exist however in terms of:

- **Recipient identification**: Finding the right Abuse Point of Contact for a notice requires understanding how the Domain Name System functions, including differences between Registries and Registrars, and between generic and country code Top Level Domains. An awareness of the existence of WHOIS and equivalent services in the ccTLD space is also needed.
- **Legitimate action**: Neither the conditions under which it is acceptable to act at the DNS level nor the type of actions that are proportionate are sufficiently understood. As a result, proper justification is often lacking, and actions requested may be technically not feasible.

Notices that are badly formulated, incomplete or lacking sufficient justification, sent to the wrong recipient, are burdensome for DNS Operators to handle and create inefficiencies. Moreover, actions to address real abuses may not be taken. Education is important to address this issue, but it requires a massive effort. Something simple could, in addition, be explored and this is the purpose of this concept note.

In this context, it is important to note that some building blocks for a solution could be used:

- For gTLDs, the Registrar Accreditation Agreement contains specific provisions (RAA 3.18), imposing on each Registrar to: "maintain an abuse contact to receive reports of abuse", whose email address "should be published on the Registrar's home page".
- The WHOIS service (irrespective of its name evolution and implementation of GDPR) already contains fields corresponding to the abuse email and phone number of the relevant Registrar.
- Work in the context of the Domains & Jurisdiction Program's Contact Group provides some clarity on criteria regarding when action at the DNS may be appropriate and formats for good notices.

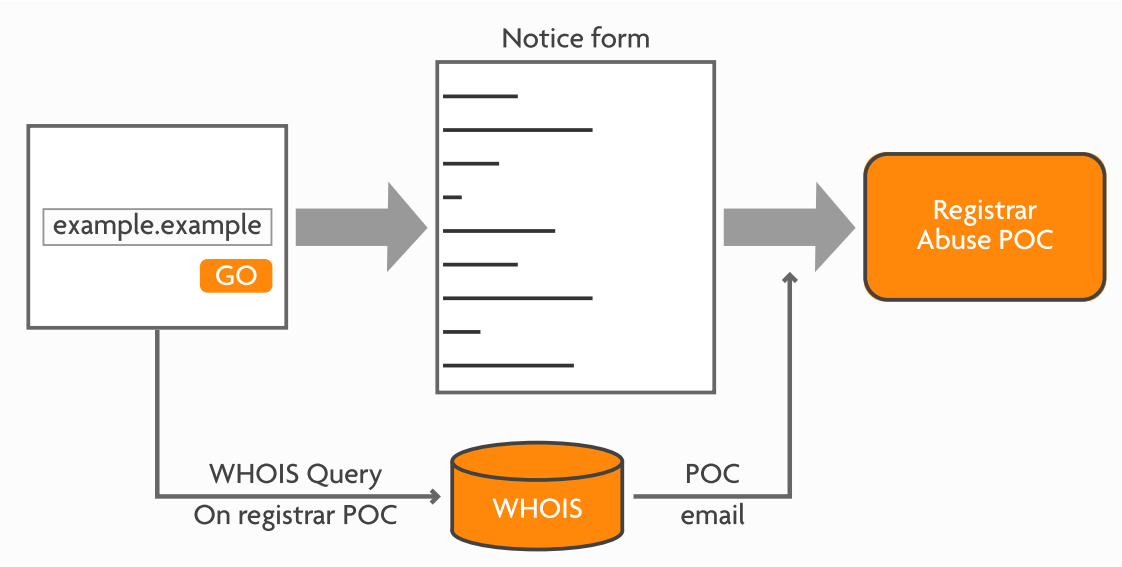
IDEA OF AN ABUSE REPORTING INTERFACE

An easy to use "abuse reporting interface" would enable sending properly documented notices to the right recipient, through:

- a targeted WHOIS query (to obtain the abuse point of contact email field), and
- a detailed form for entering technical details and justification for the notice of abuse.

A notifier would enter the targeted domain name, fill the relevant form and order it to be sent to the Registrar, as illustrated in the (highly simplified) infographic below.

This appears technically simple to implement for gTLDs. It would however require additional work to be expanded in the ccTLD space on a voluntary basis.



Leveraging the information already collected through the WHOIS service reduces the burden of maintaining accuracy of the records, in comparison to the establishment of an entirely new, dedicated database of Points of Contact.

EXPECTED BENEFITS

This proposed approach could provide the following benefits:

- Ensuring both simplicity of use for a diversity of notifiers *and* a high level of justification of notices.
- Establishing some "friction" (e.g. through compulsory fields in a form) to prevent abuse of the notice system itself and the corresponding overload.
- Clarifying the interaction channels between notifiers and DNS Operators, in an interoperable way.
- Providing an opportunity to educate notifiers on: criteria that have to be met to justify an action at the DNS level, the right DNS Operator to interact with and the procedural guarantees (including prior due diligence) that apply to them (see Criteria E - Due Diligence by Notifiers).

Additional services could be built around such an interface, including to:

- Inform the relevant registry of a notice regarding one of its domains if appropriate
- Collect useful statistics for transparency reporting.

This approach can also help a more comprehensive discussion regarding the concept of "reachability", i.e.: the conditions under which a Registrar could potentially forward a notice to a registrant (without revealing its details). This could enable, inter alia, a notifier to conduct prior due diligence.

More generally, announcement of willingness to explore such a service would represent positive public communication by the Registry and Registrar community - or at least the most engaged part of it - on its commitment to address abuses in a responsible manner, while keeping in mind the necessary protection of the neutrality of the DNS level.

NEXT STEPS

The 3rd Global Conference of the Internet & Jurisdiction Policy Network in Berlin can discuss this proposal, the potential mandate and timeline of such a group, as well as ways to ensure involvement of the most relevant stakeholders.