



INTERNET &
JURISDICTION
POLICY NETWORK

3RD GLOBAL CONFERENCE

Berlin - Germany
June 3-5, 2019

BERLIN ROADMAP



SECRETARIAT SUMMARY
AND
I&J PROGRAMS WORK PLANS



INTERNET &
JURISDICTION
POLICY NETWORK

www.internetjurisdiction.net

On June 3-5, 2019, almost 300 senior-level participants from governments, the world's major Internet companies, technical operators, civil society, academia and international organizations from more than 50 countries met in Berlin, Germany, for the 3rd Global Conference of the Internet & Jurisdiction Policy Network¹. After France (2016) and Canada (2018), this 3rd Global Conference was hosted by the Federal Government of Germany. It was institutionally supported by six international organizations: Council of Europe, European Commission, ICANN, OECD, United Nations ECLAC, and UNESCO.

The Conference marked an important milestone towards addressing key cross-border legal challenges of the digital 21st century. Stakeholders welcomed the *Operational Approaches* documents² produced in the three Programs of the Internet & Jurisdiction Policy Network: Data & Jurisdiction, Content & Jurisdiction and Domains & Jurisdiction. Prepared by dedicated multistakeholder Contact Groups, these documents contain concrete proposals for Norms, Criteria, and Mechanisms regarding respectively: cross-border access to electronic evidence, online content moderation and restrictions, and domains name suspensions. They are the result of the work of 140 Members of the three Programs since August 2018 to implement the *Ottawa Roadmap*³ adopted during the 2nd Global Conference in February 2018.

Stakeholders reiterated their strong call for the joint development in the Internet & Jurisdiction Policy Network of operational solutions and policy standards. On the basis of the concrete proposals of the *Operational Approaches* documents, participants in the 3rd Global Conference refined the *Berlin Roadmap* containing Work Plans to structure further efforts in the three Programs of the Policy Network until its 4th Global Conference in 2021.

On the occasion of the Conference, the Key Findings of the world's first *Internet & Jurisdiction Global Status Report*⁴ were formally launched. The important publication complements the policy development work in the three Programs by fostering policy coherence and enhancing capacity building around the world. 94 percent of the stakeholders from the Policy Network that were surveyed believe that jurisdictional challenges on the Internet will become increasingly acute over the next three years, while 79 percent of them state that we do not yet have sufficient coordination and institutions to address these challenges. Based on a large-scale data collection effort, the *Internet & Jurisdiction Global Status Report* aims to enable evidence-based policy innovation at global and regional levels.

After Paris in 2016 and Ottawa in 2018, this 3rd Global Conference demonstrated the commitment of a growing number of key stakeholders to engage in the work of the Internet & Jurisdiction Policy Network in order to reconcile the objectives of addressing abuses, protecting human rights and enabling the development of the digital economy.

Discussions in Berlin helped strengthen the constructive spirit manifested during the work of the Programs' Contact Groups, making this 3rd Global Conference of the Internet & Jurisdiction Policy Network a catalyzing step in the process towards jointly developing operational solutions for the common challenges of stakeholders.

¹ The list of participants, program, Stakeholder Plenary Sessions videos, and photos from the Conference can be consulted at <https://conference.internetjurisdiction.net/>

² The Operational Approaches documents can be consulted at <https://www.internetjurisdiction.net/news/operational-approaches-documents-with-concrete-proposals-for-norms-criteria-and-mechanisms-released>

³ The Outcome Document of the 2nd Global Conference of the Internet & Jurisdiction Policy Network, which contains the Ottawa Roadmap, can be consulted at <https://www.internetjurisdiction.net/news/outcomes-of-the-2nd-global-conference-of-the-internet-jurisdiction-policy-network>

⁴ More information about the world's first Internet & Jurisdiction Global Status Report can be consulted at <https://www.internetjurisdiction.net/publications/paper/internet-jurisdiction-global-status-report-key-findings>

SECRETARIAT SUMMARY

MANAGING LEGAL INTERDEPENDENCE

Day 1 of the 3rd Global Conference in Berlin highlighted the rapid evolution of the jurisdictional environment since the 2nd Global Conference in Ottawa in 2018. Stakeholders stressed the accelerated proliferation of initiatives by public and private actors. Although this is still often done in an uncoordinated manner and under the pressure of urgency, this general trend positively demonstrates a growing awareness among actors from all stakeholder groups of the common challenges they are facing and their increased commitment to address them.

Growing economic and social interdependence in our global connected society increases legal interdependence: decisions adopted in one country to regulate online activities or address abuses increasingly have extraterritorial impacts, intentionally or not; likewise, actions or inactions by internet companies have consequences for users across the globe.

This legal interdependence demands a systemic approach. It behooves all actors developing specific solutions to thoroughly assess their impact, their potential unintended consequences or negative externalities, and the longer-term dynamics they produce. Ideally, solutions should ultimately be able to scale to a large number of actors, and sufficiently adaptable to take into account future evolutions.

Even if international cooperation is under stress, participants in the 3rd Global Conference emphasized again that it is more necessary than ever. The work in the three thematic Programs of the Internet & Jurisdiction Policy Network that produced the *Operational Approaches* documents, as well as the discussions during the Conference itself were deemed illustrative of what can be achieved when actors work in a constructive spirit of mutual respect and responsible behavior.

BUILDING THE GLOBAL DIGITAL SOCIETY

Throughout history, humanity has, sometimes with conflicts, confronted the challenge of organizing itself in ever larger communities. As a result of tremendous technical innovations, we now need to manage the interactions of billions of connected people. Defining what is the digital society that we want to build, i.e. what values are sufficiently shared to potentially function at the scale of the entire humanity; and how and by whom norms should be set, implemented and enforced is nothing short of a civilizational challenge. The decisions we take today will have long lasting impacts on future generations.

Full global harmonization and uniformity is neither achievable nor desirable: it can easily negate the diversity that makes the richness of human societies. At the same time, a legal arms race among all actors to impose their own norms to the maximum extent only exacerbates conflicts and ultimately rewards the most powerful.

To avoid these extreme scenarios, stakeholders stressed the value of a third, more balanced and scalable approach, based on the fundamental principle that enabled the success of the internet as well as the World Wide Web: interoperability. Legal interoperability was therefore the central topic in the discussions of stakeholders about operational solutions and policy standards during Day 2 of the 3rd Global Conference in the Meetings of the three Programs of the Policy Network.

LEGAL INTEROPERABILITY: A PATH FORWARD

Numerous and very diverse governance regimes - public or private - set the responsibilities of the actors they apply to. Enabling interoperability and coexistence between such heterogeneous governance frameworks can reconcile the need for collective solutions with the recognition of the autonomy of actors, as well as the diversity of their cultural references and normative authority. It can provide solutions that are as distributed and scalable as the internet itself.

This requires: communication between all stakeholders to help them understand each other's situation, concerns and intentions; agreed norms of behavior to foster informal or structured coordination; and processes to develop practical cooperation mechanisms. The Internet & Jurisdiction Policy Network strives to foster such an approach via processes that engage a broad diversity of actors across stakeholder groups and regions.

Concretely, in their efforts to properly address abuses, stakeholders develop a variety of normative responses, including national laws or international agreements for public actors, or refined Terms of Service and Community Guidelines for private actors. Both types of stakeholders also plan, develop or already implement a variety of technical systems, such as platforms and portals for notifications, algorithmic tools, and technical systems to manage and respond to notices or orders. Ensuring interoperability therefore calls for a dedicated effort to address both: 1) interoperability between actors, taking into account the technical tools they employ, as well as 2) interoperability between the different applicable norms.

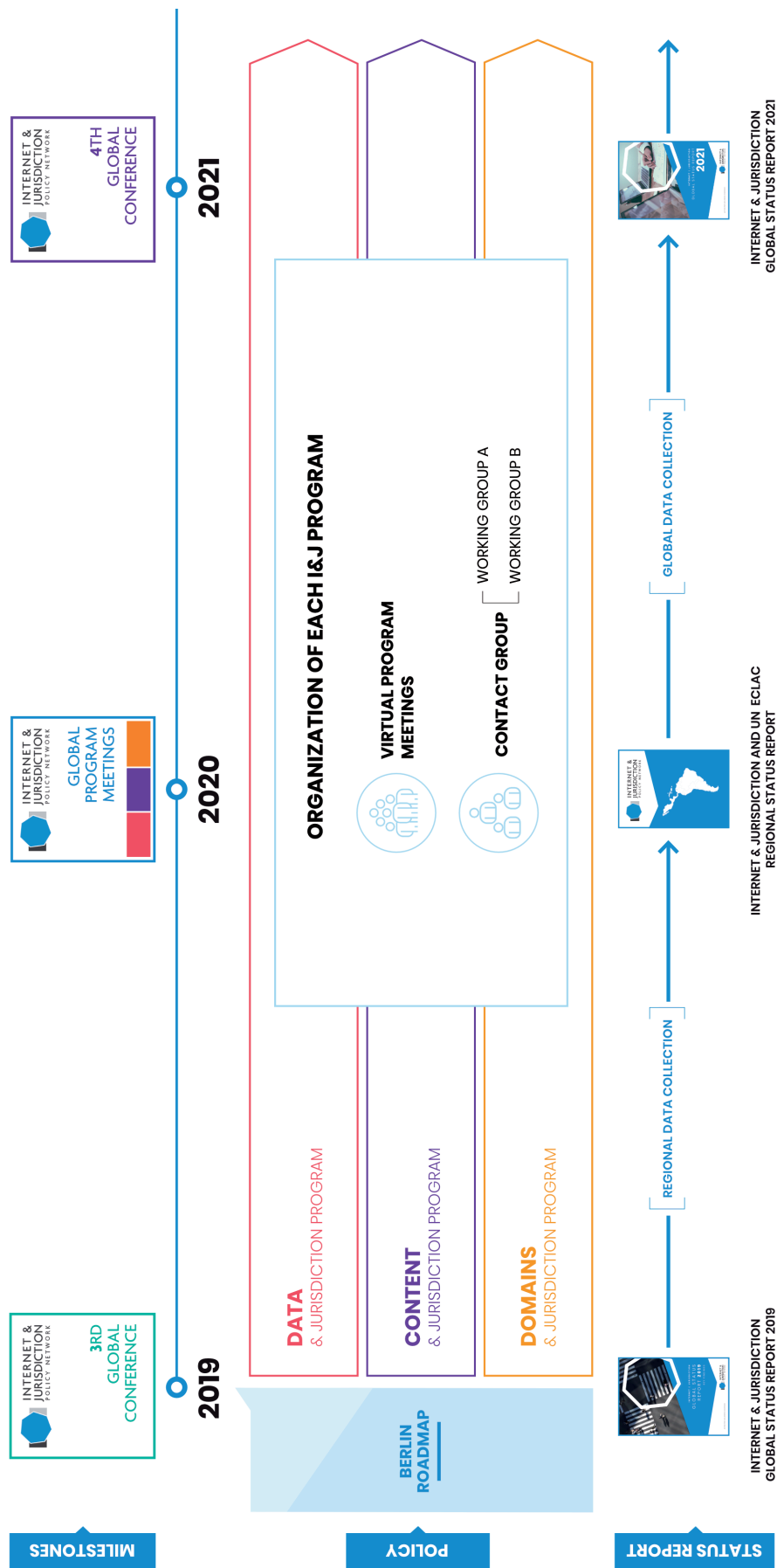
THE BERLIN ROADMAP: TOWARDS OPERATIONAL SOLUTIONS

Building on the concrete proposals for Norms, Criteria and Mechanisms of the *Operational Approaches* documents, participants in the 3rd Global Conference of the Internet & Jurisdiction Policy Network refined the **Work Plans** below to structure further work in the three Programs to advance the development of operational solutions and policy standards. .

On this basis, two first dedicated **Working Groups** will be established in each of the three thematic Programs to respectively address interoperability between actors (WG-A) and between norms (WG-B). Replicating the process established between the 2nd and 3rd Global Conferences, a Contact Group for each Program will steer and review the work of these two Working Groups.

In addition, regular **virtual Program Meetings** will be held to foster communication between Members of the Policy Network interested in the respective Programs, to provide regular updates on progress, and to explore and respond to emerging issues or specific subtopics within each Program.

As described in the timeline below, the **4th Global Conference of the Internet & Jurisdiction Policy Network** will take place in 2021, and each Program will hold a dedicated physical Global Meeting in 2020 to take stock of progress towards implementability of operational solutions and policy standards.



DATA & JURISDICTION PROGRAM WORK PLAN

CONTEXT

As stated in the Ottawa Roadmap of the 2nd Global Conference of the Internet & Jurisdiction Policy Network in Ottawa, Canada, on February 26-28, 2018:

Criminal investigations increasingly require access to information about users and digital evidence stored in the cloud by private companies in jurisdictions outside the requesting country.

Existing Mutual Legal Assistance Treaties (MLATs) procedures are broadly recognized as slow and ill-adapted. Meanwhile, limited procedural guarantees apply to direct requests sent to companies, and such direct requests can even be forbidden by some national blocking statutes.

This situation of legal uncertainty is not sustainable. In particular, the lack of clear cooperation frameworks encourages mandatory data localization approaches that are technically difficult to implement and can have detrimental impacts on the cloud economy and human rights.

Different efforts are under way to develop solutions and policy coherence between them is important: uncoordinated actions can have unintended consequences or increase conflicts of laws.

All actors are confronted with a common challenge: developing policy standards respecting privacy and due process that define the conditions under which authorized law enforcement authorities can request from foreign entities access to stored user data necessary for lawful investigations.

COMMON OBJECTIVE

In this perspective, participants in the Meeting of the Data & Jurisdiction Program at the 2nd Global Conference of the Internet & Jurisdiction Policy Network in Ottawa, Canada, on February 26-28, 2018 identified as a common objective:

The definition of high substantive and procedural standards

- Allowing relevant authorities from specific countries,
- In investigations regarding certain types of crimes with clear nexus with the requesting country,
- To directly submit structured and due process-respecting requests
- To private companies in another country to obtain the voluntary disclosure
- Of user data, irrespective of where such data is stored.

BERLIN WORK PLAN

To achieve this objective and on the basis of the Structuring Questions identified in the *Ottawa Roadmap*, the Data & Jurisdiction Program's Contact Group developed *Operational Approaches*⁵ with proposed Norms, Criteria and Mechanisms to provide a common frame of reference for all actors addressing this issue.

With this in mind, participants in the Meeting of the Data & Jurisdiction Program at the 3rd Global Conference of the Internet & Jurisdiction Policy Network in Berlin, Germany, on June 3-5, 2019 together considered and refined a draft Work Plan. This can help to guide future activities related to the Data & Jurisdiction Program, which remain focused on cross-border access to electronic evidence in criminal investigations.

Participants in Berlin underlined the importance of a strong outreach around the *Operational Approaches* document after the 3rd Global Conference. The document, organized in terms of Operational Norms, Criteria and Mechanisms, contained a great deal of useful content. Much of this reflects broad consensus that resulted from intensive discussions amongst various stakeholders, and as such, it can provide valuable input for many stakeholders addressing Data & Jurisdiction issues in various fora and processes.

At the same time, some elements in the *Operational Approaches* document were identified as warranting further attention, in some cases to clarify or better define certain aspects, in other case to explore more fully.

Participants identified the following concrete components to structure further efforts in the Program through two Working Groups dedicated to:

⁵ The Data & Jurisdiction Program Operational Approaches document can be consulted at <https://www.internetjurisdiction.net/publications/paper/data-jurisdiction-program-operational-approaches>

INTEROPERABILITY BETWEEN ACTORS (WORKING GROUP A)

This Working Group will address the procedural interfacing between requesting public authorities, service providers and other relevant parties, regarding issuance, validation, transmission and handling of requests/orders for access to electronic evidence. Participants at the 3rd Global Conference identified topics that may deserve further discussion, taking into account the progress that has been documented in the *Operational Approaches* document. Such topics include:

- **Request/order components and format** (Ref. *Criteria J – Request Formats; Criteria D-1b – Users, and Operational Mechanism – Mark-up Language and Interoperability Tags*), in particular the following subtopics:
 - Timing of notification to recipient country (prior to or concurrent with a request? Practical considerations of volume and workload?) (See also Working Group B – Interoperability of Norms)
 - Transmission of background information on the criminal investigation
 - Sufficiency of information to operationalize agreed standards, with consideration to safeguarding investigations, enabling providers' capacity to challenge requests/orders, and differentiating request components sent to judicial authorities and providers (See also Criteria J-3 and Working Group B – Interoperability of Norms)
 - Rationale for confidentiality and conditions and rationale for exceptions to user notification
 - Obligations of providers with respect to upholding of privacy standards
- **Authentication of requesting authorities** (Ref. *Criteria F-1,2,3 – Diversity of Public Authorities*)
- **Authentication of requests/orders** (Ref. *Criteria I-2,3 – Transmission*), in particular the following subtopic:
 - Possible role for competent authority (legal or judicial?) in recipient country as a point of contact (See Criteria J-3 – Request Formats)
- **Transmission channels for requests/orders** (Ref. *Criteria C – Providers, Criteria I-1,4 – Transmission, and Criteria G-1 – Diversity of Providers*), in particular the following subtopics, taking into account scalability considerations:
 - Actions of receiving competent authorities / companies
 - Timelines for responses to requests
 - Encrypted and secure transmission channels between public authorities and private actors
- **Transparency reporting on rules and statistics** (Ref. *Criteria E-1 – Transparency / Accountability*)

INTEROPERABILITY BETWEEN NORMS (WORKING GROUP B)

This Working Group will address the substantive interactions between provisions of national criminal laws and regimes enabling cross-border access to electronic evidence, under the framework of international human rights. The Working Group's work will build upon existing practice. This includes the domestic legal bases to empower competent authorities to order the production or data, and to require or permit service provider to disclose data. In addition, it includes the international legal basis for transfer of data, including aspects such as language of requests (See also Criteria J-2 – Request Formats).

Participants at the 3rd Global Conference identified topics that deserve further discussion, while taking into account the consensus amongst stakeholders documented in many parts of the *Operational Approaches*. Such topics include:

- **Types of crimes covered and their penalties** (*Ref. Criteria A-2 - Regime Scope*)
- **Judicial/independent validation of individual requests/orders** (*Ref. Criteria B-1 - Public Authorities and Criteria H-3 - Geographic Scalability*), in particular the following subtopics:
 - Responsibility for assessment of emergency situations, taking into consideration existing and developing practices (e.g., MLAT and the Budapest Convention Protocol draft provision on emergencies)
 - Duration of emergency situations
- **National standards for review and approval of a request** (*Ref. Criteria B-2,3 - Public Authorities*)
- **Clarification of and challenges to requests/orders by service providers** (*Ref. Criteria C-1,2,3 - Providers*), in particular the following subtopics:
 - Potential sanctions for non-compliance
 - Scalability issues for small providers (e.g. cost recovery, capacity)
 - Relations and distribution of roles between public and private actors in challenge processes
 - Resolution of conflicts of law
- **Safeguarding the interests of other parties than the requesting authority** (*Ref. Criteria K-3 - Nexus and Criteria E-2 - Transparency / Accountability*), in particular the following subtopic:
 - Availability/sources of resources to enhance capacities of recipient country (?)
- **User notification rules and access to remedies** (*Ref. Criteria D - Users*)
- **Elements of a request/order to be disclosed to a provider with respect to description of alleged offense** (*Ref. Criteria J - Request Formats, see also Working Group 1 - Interoperability of Actors*)

CONTENT & JURISDICTION PROGRAM WORK PLAN

CONTEXT

As stated in the Ottawa Roadmap of the 2nd Global Conference of the Internet & Jurisdiction Policy Network in Ottawa, Canada, on February 26-28, 2018:

Every day, hundreds of millions of posts and hundreds of thousands of hours of videos are uploaded on the major internet platforms and made globally accessible, greatly facilitating freedom of expression. At the same time, legitimate concerns are raised regarding increasing harmful behaviors, including hate speech, harassment, security threats, incitement to violence, or discrimination.

Protecting human rights and freedom of expression when dealing with such abuses on the internet is a major transnational challenge in the absence of clearly agreed substantive and procedural frameworks to handle the disparity of national laws: content legal in one country can be illegal in another one.

Moreover, the amount of individual restrictions decisions to be made is unprecedented, and case-by-case determinations need to carefully account for context and intent, but within very limited resources and response times given viral propagation.

In this context, opposing demands are made regarding the expectations of intermediaries: one asking them to thoroughly police content posted on their platforms to guarantee the respect of national laws and protect their users; and the other objecting to them making determinations on their own and exercising proactive content monitoring, for fear of detrimental human rights implications.

Clear common guidelines and due process mechanisms are needed to address this common challenge of all actors: maximizing the necessary remediation of harm and minimizing restrictions to freedom of expression.

COMMON OBJECTIVE

The fundamental aim is to define workable jurisdictional interfaces between disparate national legal rules. Participants in the Meeting of the Content & Jurisdiction Program at the 2nd Global Conference of the Internet & Jurisdiction Policy Network in Ottawa, Canada, on February 26-28, 2018, have agreed as a common objective the identification of the current status as well as achieving clarification and coherence with respect to the following points:

The definition of high substantive and procedural standards

- Applicable substantive norms, including the interplay between agreed international and regional human rights, national laws, and companies' community guidelines,
- The respective obligations of states and the respective responsibilities and protections of other actors, including the identification of allegedly illegal content,
- Decision-making, standards and procedures, including the escalation path for individual decisions and appeal mechanisms,
- Legitimate purposes, necessity and proportionality regarding the geographic scope of restrictions,
- The necessary due process and transparency standards that should be applied across borders.

BERLIN WORK PLAN

To achieve this objective and on the basis of the Structuring Questions identified in the *Ottawa Roadmap*, the Content & Jurisdiction Program's Contact Group developed *Operational Approaches*⁶ with proposed Norms, Criteria and Mechanisms to provide a common frame of reference for all actors addressing this issue. On this basis, participants in the Meeting of the Content & Jurisdiction Program at the 3rd Global Conference of the Internet & Jurisdiction Policy Network in Berlin, Germany, on June 3-5, 2019, identified the following concrete components to structure further efforts in the Program through two Working Groups dedicated to:

INTEROPERABILITY BETWEEN ACTORS (WORKING GROUP A)

This Working Group will address the procedural relations between public authorities, notifiers, service providers and users, as they relate to content moderation and restrictions, including in particular:

- **Formats and components of complaints from public authorities and private actors** (Ref. Criteria C-1,2 - Third-Party Notices and Criteria F - Evaluation), including mechanisms for immediacy/urgency requirements.
- **Formats and components of user notification** (Ref. Criteria I - User Notification)
- **Complaints and notification channels and tools** (Ref. Criteria C - Third-Party Notices), including mechanism for abuse of notification systems, based on post-appeal adjudication.
- **Procedures for recourse** (Ref. Criteria J - Recourse and Operational Mechanism - Approaches Pertaining to Recourse after Content Restriction)
- **Evaluation and oversight of algorithmic decision-making dealing with the procedures above** (Ref. Criteria D - Provider Detection)

INTEROPERABILITY BETWEEN NORMS (WORKING GROUP B)

This Working Group will address the interplay between international human rights, applicable national laws and international treaties, and providers' Terms of Service and Community Guidelines and their implications on the interest and rights of the user especially considering legitimate, transparent and accountable governance. The scope of the Working Group takes into account:

- **International normative coherence based on human rights** (Ref. Criteria B-2 - Normative Basis and F-1e - Evaluation)
- **Public authorities' notices on the basis of Community Guidelines** (Ref. Criteria C-1b - Third-Party Notices)
- **Geographically relevant and proportionate action** (Ref. Criteria G - Geographic Proportionality)
- **Relations between different levels of regulation of platforms and moderation on and by platforms** (Ref. Criteria B-3 - Normative Basis)
- **Normative references and jurisprudence coherence for recourse mechanisms** (Ref. Criteria J - Recourse and Operational Mechanism - Approaches Pertaining to Recourse after Content Restriction)

⁶ The Content & Jurisdiction Program Operational Approaches document can be consulted at <https://www.internetjurisdiction.net/publications/paper/content-jurisdiction-program-operational-approaches>

DOMAINS & JURISDICTION PROGRAM WORK PLAN

CONTEXT

As stated in the Ottawa Roadmap of the 2nd Global Conference of the Internet & Jurisdiction Policy Network in Ottawa, Canada, on February 26-28, 2018:

Cross-border requests for domain name suspension are increasingly sent to Domain Name System (DNS) Operators in relation to the alleged abusive content or activity on underlying websites.

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

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

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

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

COMMON OBJECTIVE

In this perspective, participants in the Meeting of the Domains & Jurisdiction Program at the 2nd Global Conference of the Internet & Jurisdiction Policy Network in Ottawa, Canada, on February 26-28, 2018 identified as a common objective to define, on a topic-by-topic basis:

The definition of high substantive and procedural standards

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

BERLIN WORK PLAN

To achieve this objective and on the basis of the Structuring Questions identified in the *Ottawa Roadmap*, the Domains & Jurisdiction Program's Contact Group developed *Operational Approaches*⁷ with proposed Norms, Criteria and Mechanisms to provide a common frame of reference for all actors addressing this issue. On this basis, participants in the Meeting of the Domains & Jurisdiction Program at the 3rd Global Conference of the Internet & Jurisdiction Policy Network in Berlin, Germany, on June 3-5, 2019, identified the following concrete components to structure further efforts in the Program through two Working Groups dedicated to:

INTEROPERABILITY BETWEEN ACTORS (WORKING GROUP A)

This Working Group will address the procedural interfacing between DNS Operators, domestic and foreign courts, specialized notifiers, individuals and registrants, and in particular:

- **Notice components and channels for abuse reporting** (*Ref. Criteria C - Notice Components and Operational Mechanism - Interface for Abuse Reporting to DNS Operators*), including the following elements:
 - Relations with law enforcement
 - Timing of responses and supporting evidence
 - Emergency routes
 - Clear go to place for information
 - Contact Information
 - Assessment / Analysis of requests
 - Globally accepted standard for request formats (and Language interfacing)
- **Mechanisms for notification to registrants** (*Ref. Criteria H - Notification to Registrants*), including:
 - Procedure for specific actors (e.g. law enforcement) to justify an exception to the principles of registrant notification
- **Procedural due diligence by specialized notifiers, and types of notifiers** (*Ref. Criteria E-2b - Due Diligence by Notifiers*), including the following elements:
 - Frameworks to identify where liability rests
 - Indemnification channels for registries
 - Role of trusted notifiers
- **Procedural aspects of recourse mechanisms for registrants** (*Ref. Criteria I - Recourse for Registrants*)
- **Notices traceability and statistics collection** (*Ref. Criteria G-1 - Transparency*), including the following elements:
 - Process transparency
 - Data relevant to process transparency
- **Expectations of parties in an abuse reporting system** (*Ref. Criteria C - Notice Components and Operational Mechanism - Interface for Abuse Reporting to DNS Operators*)

⁷ The Domains & Jurisdiction Program Operational Approaches document can be consulted at <https://www.internetjurisdiction.net/publications/paper/domains-jurisdiction-program-operational-approaches>

INTEROPERABILITY BETWEEN NORMS (WORKING GROUP B)

This Working Group will address the interaction between national laws, DNS Operators' policies, and specialized notifiers' rules, in particular:

- **Thresholds justifying action, according to different types of abuse** (*Ref. Criteria A - Types of Abuse and Criteria B - Thresholds*), including the following elements:
 - Mapping of the normative source of harms and of current thresholds for action by DNS Operators
 - Principle of proportionality and exhaustion of alternative measures
 - Collective interest of consumers
 - Severity of abuse/harm and associated channels of notification and escalation
 - Assessment of the registrant's knowledge of the abuse
- **Geographic reach of court orders from the DNS Operator's country of incorporation** (*Ref. Criteria D-1 - Notifier Types*), including:
 - Risk of local action having global effects
- **Handling of court orders from outside the jurisdiction of the DNS Operator** (*Ref. Criteria D-2a - Notifier Types*), including:
 - International normative consistency (including differences in consistency between technical abuse and content abuse)
- **Substantive due diligence by Notifiers** (*Ref. Criteria E-2a - Due Diligence by Notifiers*), including the following elements:
 - Potential impact on other actors due to the specific nature of the DNS
 - Roles and descriptions of trusted notifiers
 - Potential role of artificial intelligence in making decisions
 - Identification of the DNS Operator by the notifier