GLOBAL INTERNET AND JURISDICTION CONFERENCE 2018

FEBRUARY 26-28 • OTTAWA, CANADA

TOWARDS POLICY COHERENCE AND JOINT ACTION

SUMMARY BY THE SECRETARIAT OF THE INTERNET & JURISDICTION POLICY NETWORK AND OTTAWA ROADMAP

INTERNET & JURISDICTION POLICY NETWORK

www.internetjurisdiction.net

TOWARDS POLICY COHERENCE AND JOINT ACTION

Secretariat Summary and *Ottawa Roadmap*

Second Global Conference of the Internet & Jurisdiction Policy Network

Ottawa, Canada, February 26-28, 2018

I. SECRETARIAT SUMMARY

On February 26-28, 2018, over 200 senior-level participants from governments, major Internet companies, technical operators, civil society, academia and international organizations from more than 40 countries met in Ottawa, Canada, for the second Global Conference of the Internet & Jurisdiction Policy Network.

Building on the results of the first Global Conference in November 2016 in Paris, France, and subsequent intersessional work, the second Global Conference focused on the definition of *Work Plans* with common objectives and structuring questions to develop concrete solutions to pressing jurisdictional challenges on the internet.

Organized in partnership with the Government of Canada, the Conference was institutionally supported by the OECD, the Council of Europe, UNESCO, the European Commission and ICANN. A high-level Advisory Group supported the Secretariat's preparatory process.

The innovative format eschewed formal panels to enable a high degree of interactions. Between the Stakeholder Plenary Sessions on Days 1 and 3, in-depth discussions were carried out on Day 2 in parallel Workstreams corresponding to the three Programs of the Policy Network: Data & Jurisdiction, Content & Jurisdiction, and Domains & Jurisdiction.

The Conference sent important messages and established a clear roadmap to structure further work in the lead-up to the third Global Conference of the Internet & Jurisdiction Policy Network, to be held in Berlin in June 2019, in partnership with the Government of Germany.

THE DANGERS OF LEGAL UNCERTAINTY IN CYBERSPACE

On Day 1, participants reiterated their concerns regarding jurisdictional tensions on the internet and the resulting high degree of legal uncertainty. This increases the cost of doing business, brings challenges for governments to protect their citizens and ensure respect of their legislations, and raises civil society concerns that abuses are not properly addressed or that solutions will harm users.

Patching actions, taken in a reactive mode under the pressure of urgency, produce a legal arms race with potentially detrimental impacts on the cloud economy, cybersecurity and human rights. This risks increasing the degree of legal uncertainty, instead of reducing it.

THE FUTURE OF THE DIGITAL SOCIETY IS AT STAKE

The lack of clear transnational cooperation frameworks prevents addressing crime, harassment, incitement to violence and numerous other harmful behaviors affecting citizens in their everyday life. In this context, participants are united in their commitment to reconcile the three objectives of fighting abuses, protecting and promoting human rights, and enabling the development of the digital economy.

What is needed is defining the rules applying to cross-border communities of hundreds of millions of people with increasingly diverse cultural or social references; ensuring the coexistence of numerous different legal frameworks in cyberspace; and clarifying the respective responsibilities of the different stakeholders in that regard. What is at stake is the collective definition of the digital society we want to build, and the development of governance mechanisms to prevent the deepening of existing lines of fracture.

THE NEED FOR FRAMEWORKS

The concrete challenges addressed at the Conference were based on the *Areas for Cooperation* agreed upon at the first Conference in 2016[1]. The Ottawa Conference moved past problem framing to concretely discuss policy options and components of solutions. Participants highlighted the importance of approaching these issues through the development of cooperation frameworks and standards for interoperability.

Addressing these issues however, participants reiterated in Ottawa, can only be achieved through cooperation among all stakeholders.

ENSURING POLICY COHERENCE

The cost of past inaction has been dire, but so would be uncoordinated efforts going forward.

In recent months, public and private entities around the world announced and adopted different initiatives to address the issues at stake. They touch upon very sensitive topics, including the territorial reach of national legislations and the responsibilities of private actors. In this context, a major challenge is to ensure that the multiplication of different regimes does not create additional tensions, or even conflicts, and that legal interoperability between those regimes is established.

It was highlighted that particular attention should be given to, inter alia: how such regimes should handle diverse categories of intermediaries; the potential unintended transborder impact they may have; their capacity to scale geographically; and the long-term consequences if they were generalized and widely adopted.

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

THREE WORK PLANS FOR JOINT ACTION

On Day 2 of the Conference, stakeholders worked together in three parallel Workstreams under Chatham House Rule. Corresponding to the three Programs of the Policy Network, these focused respectively on:

- **Workstream 1:** Cross-border access to user data
- **Workstream 2:** Cross-border content restriction
- **Workstream 3:** Cross-border domain suspension

Three Policy Options Documents[2] served as official input in the discussions. They presented the results of the intersessional work of dedicated multistakeholder Contact Groups set up after the first Global Conference of the Policy Network in Paris.

On this basis, participants jointly reviewed and refined the Work Plans included below. Each *Work Plan* formulates concrete common objectives that stakeholders set for themselves, and defines a clear list of structuring components for the development of operational frameworks. These structuring components will guide the multistakeholder policy development work facilitated by the Secretariat after the Ottawa Conference. They will also enhance coordination and policy coherence between respective efforts undertaken by participants in the Policy Network.

A ROADMAP TOWARDS BERLIN

The second Global Conference of the Internet and Jurisdiction Policy Network represented a major milestone in its ongoing policy development process initiated in 2012 and accelerated by the first Global Conference in 2016. Building on the success of the subsequent intersessional work conducted in 2017, the second Global Conference further strengthened the momentum for cooperation among all actors. The results of the three Workstreams provide a clear roadmap towards the third Global Conference, to be held in Berlin on June 3-5, 2019, in partnership with the Government of Germany.

In the final Stakeholder Plenary Session on Day 3, participants highlighted the importance of the work that must be conducted without delay and their commitment to engage in it, including through the Working Groups that will be set up for that purpose, as indicated in the Timeline below.

This session also highlighted the importance of reporting by the Secretariat on the outcomes of the Conference to relevant international processes, and of outreach to various communities to ensure inclusion and broad awareness.

The list of participants, program, Stakeholder Plenary Sessions videos, and photos from the Conference can be consulted at https://conference2018.internetjurisdiction.net/.

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

II. OTTAWA ROADMAP

The three following *Work Plans* - for each of the three Programs of the Internet & Jurisdiction Policy Network - were reviewed and refined by the participants in the respective Workstreams of the second Global Conference of the Internet & Jurisdiction Policy Network in Ottawa. These *Work Plans* will structure further work towards the third Global Conference on June 3-5, 2019, in Berlin, Germany.

DATA & JURISDICTION PROGRAM
WORK PLAN

Criminal investigations increasingly require access to information about users and digital evidence stored[1] 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.

OBJECTIVE

In this perspective, participants in the Data & Jurisdiction Workstream at the second 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.

[1] The focus here is on cross-border access to stored data. Interception and encryption are not directly addressed and require separate discussions.

STRUCTURING QUESTIONS

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

1. **Standards:** Statutory requirements to ensure high and robust human rights protections, while meeting lawful requests from law enforcement, and providing legal clarity to those receiving requests.
2. **Qualifying regimes and requests:** Streamlined access to data requires both a qualifying regime and qualifying individual requests.
3. **Countries:** Evaluation and review procedures to determine eligible countries, while seeking to improve practice for requests to all countries.
4. **Authorities:** Competent authorities, defined by nation or for units within a nation, for issuing cross-border requests.
5. **Scope:** Types of criminal investigations to be considered within scope.
6. **Nexus:** Elements allowing a requesting country to demonstrate its substantial connection and legitimate interest in the data stored by the foreign provider.
7. **Users:** Provisions regarding users who are not nationals or residents of the requesting country.
8. **Requests:** Content and structure of properly documented requests, with proper legal authorization, including judicial approval where possible.
9. **Due process:** Guarantees regarding, inter alia: user notification, capacity to object, recourse and redress. Consideration of notice to relevant non-requesting nations.
10. **Companies:** Voluntary nature of disclosure (although similar factors apply to compulsory regimes) and procedures in case of doubt.
11. **Data:** Tailored rules for categories of data, such as content and non-content data, or for especially sensitive information.
12. **Data location:** How to deal with data stored digitally, providing weight to factors beyond its physical location.
13. **Scalability:** Framework extension over time, beyond initial participating countries, to respond to increasing magnitude and diversity of requests.
14. **Data preservation:** Provisions to preserve data for an individual investigation, before a full request for data can be made.
15. **Capacity:** Providing training and staffing to meet the regime's requirements.

CONTENT & JURISDICTION PROGRAM
WORK PLAN

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.

OBJECTIVE

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

- 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.

STRUCTURING QUESTIONS

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

1. **Standards:** Addressing conflicts of different substantive norms to identify allegedly illegal content and determining the relationship/hierarchical nature of the relationship.
2. **Convergence:** Level of global convergence achievable or desirable in such definitions.
3. **Response time:** Appropriate reaction delays by intermediaries after reception of notices.
4. **Decision-making:** The architecture of decision-making and the role of different types of state and non-state actors (including intermediaries, governments, courts, regulators, and individuals that file requests).
5. **Algorithms:** Appropriate combination of algorithmic tools and human review considering the limits of algorithmic tools.
6. **Procedural Standards:** Procedural standards assessing the legality of content: assessment standards, assurance and verification, roles and remedies.
7. **Geographic scope:** Situations - if any - that could, as a matter of exception from local filtering, justify global restrictions, including measures that address contradictory actions by different states.
8. **Transparency:** Expanding existing efforts and strengthening coordination among them.
9. **Request formats:** Documenting and circulating what proper [government] requests should contain.
10. **Notification:** Handling of notification of users and their capacity to object.
11. **Remediation**: Mechanisms for the prompt restoration of abusively restricted content.
12. **Types of content:** Characteristics of content including intention and possible effects; determining appropriate measures for addressing different types of content.
13. **Types of actors:** roles and responsibilities

DOMAINS & JURISDICTION PROGRAM
WORK PLAN

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

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

Acting at the DNS level should only be considered when it can be reliably determined that 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 distinctions between country-code and generic Top Level Domains in terms of relations with, respectively, ICANN and national laws or authorities, lead to very different approaches and constraints.

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

OBJECTIVE

In this perspective, participants in the Domains & Jurisdiction Workstream at the second 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:

- 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.

[1] This exercise focuses on abusive content, not registration or infrastructure abuse, although aspects discussed here can also relate to the latter.

STRUCTURING QUESTIONS

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

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

TIMELINE OF THE INTERNET & JURISDICTION POLICY NETWORK UNTIL 2019