INTERNET & JURISDICTION
A GLOBAL MULTI-STAKEHOLDER DIALOGUE PROCESS

ENABLING MULTI-STAKEHOLDER COOPERATION

STATES | INTERNET PLATFORMS | TECHNICAL OPERATORS | CIVIL SOCIETY | ACADEMIA | INTERNATIONAL ORGANIZATIONS

Contribution to the expert meeting "Jurisdiction in Cyberspace" Amsterdam, March 6-8, 2016

Please find below some elements based on the dialogue process facilitated since 2012 by the Internet & Jurisdiction Project, and related to:

- "Situations in which mutual legal assistance is ineffective, because of legal differences between countries, or time consuming mutual legal assistance processes"; and
- "Conflicting regulations hamper cooperation with private parties"

1 - Time consuming processes

This is a major criticism towards the MLAT system. Obtaining information usually requires several months (for non-emergency cases) and sometimes up to two years. This makes the system irrelevant for most investigations and discourages the use of the mechanism in the first place.

One reason is the limited human and financial resources in the recipient countries' services dealing with requests, while the number of requests has significantly increased (+ 1.000% in the last decade for the US). Additional resources are clearly necessary, yet hard to obtain in situations of budgetary restrictions.

The second reason for delays is the multiplicity of steps involved in the processing of requests, inside both requesting and requested countries. As they are intended to provide procedural guarantees, removing any of these steps represents a complex endeavor, akin to process reengineering, that actors are very cautious about. Streamlining existing procedures only go so far. Yet, anecdotal evidence shows that some delays are due to internal procedures of sending countries, which can be streamlined more easily than those of receiving ones.

Reduction of delays could focus on two key complementary approaches:

- Digitization of Workflow. The entire process should move towards full electronic transmission chains: contrary to widespread belief, significant progress has already been done in that direction but it should be intensified. Some technical Legal Cooperation Protocol could be envisaged.
- Standard Request Format(s). Incomplete or sketchy requests lead to back-and-forth demands for additional information, lengthening the process and making the ultimate acceptance of the request less likely. The creation of standard request format(s) - potentially specific to each type of request - would greatly simplify the workflow and create interoperability. Such format(s) would compel requesters to provide key pre-agreed elements. From the Internet & Jurisdiction process, the following components for Standard Request Formats emerged (non exhaustive list):
    - authenticated identification of senders and recipients
    - reference to clear local legal basis
    - the national procedure followed,
    - specificity,
    - explicit and detailed allegation
    - justification of necessity and proportionality
    - criteria for potential emergency and confidentiality

  Such format(s) would help implement so-called "due process by design".

2 - Situations of legal differences

Given the global nature of online services, cross-border interactions become the norm rather than the exception: globally available content can be legal in some countries but illegal or even criminal in others; and the ubiquity of communication devices makes the cross-border collection of digital evidence an essential part of almost any criminal investigation. In both cases, the Internet platforms or technical operators are often in a different country than where content is posted or a crime was committed.

Most – although not all – MLA treaties require "dual incrimination", ie: that the alleged behavior be considered criminal in both the requesting and requested countries. This is intended to ensure citizens the protection of the highest standard of both countries. But substantive and procedural legal disparities between countries make traditional legal assistance mechanisms ineffective.

Moreover, regardless of the actual physical location of events or involved parties, this de facto imposes the law of the recipient country over the law of the requesting one. Given the dominant role of US-based companies, many countries resent this asymmetry when the only connection to the US is the use of an online service incorporated in its territory. Measures such as blocking of entire platforms or compulsory data localization might proliferate as a result and solutions are needed for both content takedowns and access to user data.

Content takedowns.

Online platforms initially imposed upon their users the jurisdiction of their country of incorporation, but courts have progressively established that local laws should also apply. In situations of substantive divergence of legislations regarding content, no transnational procedures yet exist to address this issue. Companies have developed detailed global Community Guidelines regulating what users can post, with significant convergence in recent years around clauses covering for instance - in various formulations - hate speech, incitation to violence and discrimination. In parallel, foreign public authorities increasingly send global platforms direct requests for removal of content illegal in their respective territories and the practice of partial withholding (in particular via geo-IP filtering or ccTLD-based country lenses) has developed. However, this approach remains ad hoc, without sufficient transparency, due process and scalability. Discussions in the context of the Internet & Jurisdiction Project in the past years indicated a possible avenue forward, via the development of due process frameworks structured around the following elements:

Request submission

- Standardized formats with mutually agreed compulsory elements
- Authentication mechanisms for senders, taking into account local authority chains and procedures
- Legal clarity on applicable national laws and procedures
- Transparency reporting from by both public and private actors, in commonly agreed and comparable formats

Request handling

- Shared procedural norms and decision-making criteria, including shared vernacular
- Advisory and reference bodies for situations of ambiguity
- Appeal and redress mechanisms for users across borders
- Public-private dialogue channels in situations of escalating tensions

Cross-border access to user data

Access by law enforcement to user data stored by Internet companies is becoming critical for most criminal investigations. Given the major role of US-based companies, this raises two complementary challenges.

First, should data held by US companies be generally accessible to US law enforcement, irrespective of where it is stored, whom it concerns and where the alleged crime took place? The issues at stake touch upon the extra-

territorial extension of sovereignty in cyberspace, privacy protection and the debate around data localization. A major lawsuit is currently ongoing regarding emails stored by Microsoft on Irish servers in the context of a US investigation of a drug crime. Pending decision on this case, which is likely to take some time, legal uncertainty prevails. Discussions are needed to explore whether some set of criteria could be developed to frame the conditions of access by law enforcement in one country to data stored by operators located in their territory that may relate to foreign citizens. This is of course relevant for US-based platforms, but similar issues regard Internet operators based in other countries.

The second issue is access by foreign governments to user data stored by US companies when the only nexus of connection with the US is the use of such operators, while the crime, the alleged perpetrator(s) and victim(s) have no connection to the US. Significant work has already been conducted in the US by a working group of companies, civil society and academics to explore a possible exception to the Electronic Communications Privacy Act (ECPA). It would allow, under certain strict conditions, requests by accredited foreign governments to be sent directly to US-based companies to access the content of such communications – and not only the metadata as currently allowed by ECPA. Significant issues remain to be clarified to ensure both the highest respect of human rights protections and efficiency, but this US initiative constitutes a serious discussion basis. It should be explored further, with stronger involvement of actors outside of the US, in Europe and elsewhere, which have not so far been part of the discussions.

3 - Necessary ongoing multi-stakeholder dialogue(s)

The MLAT system could be qualified as the "switched network of international cooperation". In particular, this system of mostly bilateral treaties does not scale well. As the Internet develops to four or five billions of users and operators become located in more and more countries, these cross-border challenges will only expand. Many countries do not have MLATs with each other and developing such tools among 190 countries would require more than 18.000 agreements. More scalable (ie: generic) solutions are needed.

Another situation that remains to be addressed is when, even if the conflict does not directly connect with the country of incorporation of the operator, it still involves multiple jurisdictions. For example if content posted legally in country A through a platform incorporated in country B is illegal in country C; or if a crime involves countries A and B, an Internet platform incorporated in country C, and potentially its servers in country D.

Ensuring that in the long-term a solution can scale up to more than a few countries and addressing such complex situations requires transnational "policy standards" to establish procedural interoperability between heterogeneous actors and due process across borders. Otherwise, a legal arms race could threaten the very nature and benefits of the cross-border Internet, without addressing its misuse.

None of the above issues however can be solved by any category of actors alone. Ongoing multi-stakeholder dialogues need therefore to be facilitated and financially supported, in order to develop innovative cooperation frameworks that are as transnational as the Internet itself.

About the Internet & Jurisdiction Project

The Internet & Jurisdiction Project facilitates since 2012 a pioneering global multi-stakeholder process to address the jurisdictional tensions produced by the cross-border nature of the Internet. It actively engages over 100 key entities around the world including: states, Internet companies, technical operators, civil society and international organizations and is supported by the I&J Observatory, an expert-network of 30+ leading academics. To allow the digital coexistence of diverse national laws in shared cross-border online spaces and prevent a legal arms race detrimental to all, the Internet & Jurisdiction Project helps stakeholders develop transnational cooperation mechanisms that guarantee due process across borders.