INTERNET & JURISDICTION POLICY NETWORK

DATA & JURISDICTION

WORK PLAN

This Work Plan was reviewed and refined by stakeholders gathered on February 26-28, 2018 in Ottawa, Canada for the 2nd Global Conference of the Internet & Jurisdiction Policy Network. Taking stock of the outcomes of the 1st Global Conference in 2016 in Paris, and the intersessional work conducted in 2017, this document will guide the work in the Data & Jurisdiction Program of the Policy Network in preparation for its 3rd Global Conference, which will take place in Berlin, Germany, on June 3-5, 2019.

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

.

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

Objective

In this perspective, participants in the Data & Jurisdiction Workstream at the second Global Conference of the Internet and 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.

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 for 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.