WS87, "Law Enforcement, Cyberspace & Jurisdiction", 7 December, 12:00-13:30

Session Title	Law Enforcement, Cyberspace & Jurisdiction
Date	7-12-2016
Time	12:00-13:30
Session Organizer	Computer & Communications Industry Association (CCIA) & Council of Europe
Chair/Moderator	Christian Borggreen (CCIA)
Rapporteur/Notetaker	Bijan Madhani (CCIA)
List of Speakers and their institutional affiliations	- Alexander Seger, Head of Cybercrime Division, Council of Europe - Neide de Oliveira, Coordinator of the National Working Group on Cybercrime, Brazil - Paul Mitchell, General Manager, Technology Policy, Microsoft Corporation - Bertrand de la Chapelle, Director, Internet & Jurisdiction Project - Emma Llanso, Director of the Free Expression Project, Center for Democracy & Technology - Nathalia Foditsch, American University
Key Issues raised (1 sentence per issue):	Law enforcement access to evidence stored in the cloud.
If there were presentations during the session, please provide a 1-paragraph summary for each Presentation	Christian Borggreen introduced the panel aimed at discussing the challenges identified by main stakeholders on law enforcement access to e-evidence; national, regional and global solutions for cooperation; and ways to avoid the fragmentation of cyberspace. Neide de Oliveira, Coordinator of the National Working Group on Cybercrime, Brazil, provided an update on the situation in Brazil where rules on cyber evidence are based on the Marco Civil law. Brazil's government can mandate local data storage for services used by Brazilians. The government can also block for communication services deemed uncollaborative. Internationally, Brazil is advocating for more cooperation on Mutual Legal Assistance Treaties (MLATs). Paul Mitchell, General Manager, Technology Policy, Microsoft Corporation, drew attention to the interplay between national and international law, pointing to the ongoing dispute between Microsoft and the US Government over whether U.S. prosecutors can gain access to emails stored in Ireland. Despite these controversial cases there are frameworks today for international cooperation (e.g. Microsoft responded to email data requests related to the Charlie Hebdo attacks in 47 minutes). Yet, when dealing with data requests in one country, operators often face the problem of conflicting laws. Nathalia Foditsch, American University, presented the cost and limitations of recent law enforcement actions.

	On average, it takes about 10 months to get a reply to an MLAT request. Yet, when discussing alternatives to the MLAT system, what needs to be taken into account is to extent to which proposals might foster further privatisation in the governance of the Internet. Among the dangers she listed were data localisation mandates and government hacking risks. Emma Llanso, Director of the Free Expression Project, Center for Democracy & Technology, made a case for the importance of transparency in trans-border data flows not only for users, but also for governments and companies. Transparency enables accountability and individual empowerment and helps inform policy discussions and advocacy. She referred to the recent report of the Freedom Online Coalition Working Group on the state of play around data transparency. A major challenge to fostering transparency is the scale of the big data management project and the classification of data to make public. Bertrand de la Chapelle, Director, Internet & Jurisdiction Project, talked about their conference in Paris last month on cross-border access to user data. In his opinion, it is important to foster policy coherence, first by developing standards and processes for access to basic subscriber information. Establishing jurisdiction is particularly difficult: should it be the location of the server or of the company that counts when data requests are made? De la Chapelle argued that neither is optimal, and more criteria should be taken into account, such as the location of the crime or the nationality/residence of the person whose data is requested. Among the areas for cooperation to be explored are: criteria for determining jurisdiction, due process mechanisms and harmonisation of standards on user notification. Alexander Seger, Head of Cybercrime Division, Council of Europe, provided an overview of the solutions under discussion in the framework of the Budapest Convention on Cybercrime. The convention has 50 parties and 17 observer states. It has a working group on cloud evidence, established 2 years ago, which recently released a set of recommendations. 'Without data, there is no evidence, there is no justice', said Seger. The challenges around subscriber data, loss of knowledge of location and enhanced European regulations as of April 2018 were also mentioned.
Please describe the Discussions that took place during the workshop session: (3 paragraphs)	The presentations and subsequent discussion were based on four shared goals for reforming law enforcement access: 1. Improve efficiency of lawful government requests.

	2. Reduce government incentive for "problematic" direct access to data (e.g. forced data localisation or direct requests which may put companies in conflict of national laws). 3. Transparency and clarity for users, governments, and companies. 4. A framework for cross-border data requests which protects users' rights. Main comments included: • The current jungle of legal processes is unworkable for law enforcement, companies and users; • Emphasise training of judges and clarify the interpretations and intentions of laws; • Governments should consider other penalties, e.g. economic, rather than interrupting communication services (which in Brazil blocked 100 million users); • In establishing jurisdiction, do not focus solely on the location of the data, but also on the person in possession or control as the key factor; • There is no single actor or group of actors that can solve the problems of Internet and jurisdiction in the policy network; • Need to foster real dialogue e.g. between prosecutors and companies to elicit cooperation while remembering that service providers must answer to the laws of their own lands; • Avoid forum shopping. • Consider allowing companies to respond directly to foreign government requests; • Be aware of which standards apply in which jurisdictions.
Please describe any Participant suggestions regarding the way forward/ potential next steps /key takeaways: (3 paragraphs)	In conclusion, the panelists each made one suggestion for future focus, which included: • Due process across borders; • Seek agreement on treatment of cross border issues; • Overview of how national laws interact with the digital age; • Ensure participation of wider society in the debate; • Increase privacy protections and transparency.

	In 2017 both the Council of Europe and in the European Union will present specific actions which could be presented and discussed at next year's IGF.