WS 149 „Crime and Jurisdiction in Cyberspace: Towards Solutions“, 20 December 2017, 15:00-16:30

Session Title	Crime and Jurisdiction in Cyberspace: Towards Solutions
Date	20-12-2017
Time	15:00-16:30
Session Organizer	Computer & Communication Industry Association (CCIA) & Council of Europe
Chair/Moderator	Christian Borggreen (CCIA)
Online Moderator	Pierluigi Perri (University of Milan)
Rapporteur	Andrea Candrian (Federal Office of Justice, Switzerland)
List of Speakers and their institutional affiliations	- Priscila Schreiner, Federal Prosecutor Office, Brazil - Paul Mitchell, Microsoft - Seth Bouvier, US State Department - Gregory Nojeim, Center for Democracy & Technology - Paul Fehlinger, Internet&Jurisdiction - Cathrin Bauer-Bulst, European Commission - Alexandru Frunza-Nicolescu, Council of Europe
Summary for each presentation	Christian Borggreen introduced the panel and emphasized the fact that issues such as cloud computing raise a number of questions for criminal investigations. Often, conflicts may arise between different national legislations. Uncertainty and legal discrepancies for authorities and industry involved may be one result. Frustration among law enforcement authorities is spreading, and costs as a consequence of the shutdown of applications and sites are more than considerable. The need to follow up on the Workshop organized by CCIA& Council of Europe held in Mexico last year is obvious. Priscila Schreiner gave an insight view into the legal approaches regarding the fight against cybercrime in Brazil and respective criminal proceedings. The issue whether an ISP is offering its services in the country or whether it has established its headquarters or a local branch on that territory may be decisive with regard to the legal possibilities and competences of investigating authorities. The speaker pointed out that, in that context, encryption should not be regarding solely as an obstacle to law enforcement, but as a necessary tool in electronic communication. Paul Mitchel took up the issue of the Microsoft/US DOJ case regarding email data stored in Ireland which be

	decided by the US supreme court. He pointed out the concurring, but not necessarily conflicting interests and rights of industry, customers and States. It is essential for all parties involved that clarity be provided regarding their rights and obligations as well as regarding the rules governing national and international cooperation. Seth Bouvier pointed out the vast increase of requests for information (from national law enforcement authorities and from abroad). A complicated and resource demanding process of back and forth must be avoided. Instead, MLAT procedures should be improved. Regarding the envisaged US/UK agreement on the sharing of data for law enforcement purposes, the speaker confirmed that there might well be a possible impact regarding other countries, as well, once the agreement has been put into practice and evaluated. Greg Nojeim raised the issue of legislations dealing with the exchange of data and information and with international cooperation in this context. Existing shortcomings relating for example to data protection or the rule of law should be detected and eliminated. Concepts such as proportionality, specificity, the restriction to serious criminal cases or systematic verification that there is no less intrusive measure available are essential safeguards, in this regard. Paul Fehlinger emphasized the need to come up, among all stake holders, with coherent strategies by mapping, analyzing and comparing different strategies and approaches regarding crime and jurisdiction in cyberspace. This will provide us with real policy options that enable us to lead further discussions on a necessary solid basis. Cathrin Bauer-Bulst pointed out the fact that, while economy, politics, markets and societies as such are opening up towards each other, the means and instruments of criminal jurisdictions do not. She elaborated on different approaches in order to enhance and speed up cooperation in this context, for example digitalization of communication between authorities involved, training and instruction of staff or single points of contact regarding the exchange of specific categories of data. Alexandru Frunza-Nicolescu presented the Council of Europe's perception of the challenges regarding jurisdiction in cyberspace und the actions undertaken by the organization: Beside the relevant Budapest Convention on Cybercrime and the continuing work and efforts in this context (by striving towards an additional protocol), he specifically pointed out the efforts in the field of capacity building projects that have become a relevant tool worldwide. More effective MLA proceedings, direct cooperation between authorities and ISPs and a

	clearer framework regarding strong safeguards are key to a successful approach in the context of cybercrime.
Discussions during the workshop	It was reiterated that technological developments should never pose an insurmountable impediment to law enforcement and international cooperation in this regard. The existence of a community of thrust between different players and partners in the joint fight against cybercrime is the ultimate challenge and objective, while ensuring and strengthening established safeguards.
Way forward	All stakeholders should continue to work together, while respecting and protecting the rights of individuals and the States as well as the needs of industry as a solid basis for economic development and growth. National and international efforts to strengthen and improve instruments in the fight against cybercrime should be combined, whenever feasible, with the principle of transparency. Early publication of texts, agreements and drafts should be envisaged, allowing for discussion in and contributions from a wider audience.