HEMISPHERIC FORUM ON INTERNATIONAL COOPERATION AGAINST CYBERCRIME
Santo Domingo, 5-7 December 2017

Access to evidence in the cloud (Introduction to workshop 5)

Alexander Seger
Council of Europe
alexander.seger@coe.int

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Cybercrime and electronic evidence: Challenges for criminal justice

- The scale and quantity of cybercrime, devices, users and victims
- Technical challenges (VPN, anonymisers, encryption, VOIP, NATs etc.)
- Cloud computing, territoriality and jurisdiction
  - Cloud computing: distributed systems ▶ distributed data ▶ distributed evidence
  - Unclear where data is stored and/or which legal regime applies
  - Service provider under different layers of jurisdiction
  - Unclear which provider for which services controls which data
  - Is data stored or in transit ▶ production orders, search/seizure or interception?
- The challenge of mutual legal assistance
- No data ▶ no evidence ▶ no justice

Crime and jurisdiction in cyberspace ► Issues and solutions under the Budapest Convention on Cybercrime

Specific issues to be addressed:

- Differentiating subscriber versus traffic versus content data
- Limited effectiveness of MLA
- Loss of location and transborder access jungle
- Provider present or offering a service in the territory of a Party
- Voluntary disclosure by US-providers
- Emergency procedures
- Data protection

Example: voluntary cooperation by providers

	Requests for data sent to Apple, Facebook, Google, Microsoft, Twitter and Yahoo in 2015		
Parties	Received	Disclosure	%
Austria	254	119	47%
Belgium	1 992	1 453	73%
Canada	1 157	884	76%
France	27 213	14 746	54%
Germany	29 092	15 469	53%
Italy	7 847	3 591	46%
Netherlands	1 605	1 213	76%
Poland	2 378	820	34%
Portugal	3 255	1 751	54%
Spain	4 151	2 092	50%
United Kingdom	29 937	21 075	70%
USA	89 350	70 116	78%
Total excluding USA	**138 612**	**82 529**	**60%**
Total including USA	227 962	152 644	67%

Example: voluntary cooperation by providers

2016	Facebook			Microsoft	
	Requests sent	Data received	Preservation requests	Requests sent	Data received
Argentina	1804	75%	868	1414	80%
Bahamas	2	0%		0	
Barbados	3	0%		0	
Brazil	3562	52%	2101	2471	38%
Chile	760	40%	64	226	75%
Costa Rica	8	20%	175	127	65%
DomRep	175	51%	93	13	75%
Mexico	1135	75%	99	584	70
Panama	11	45%	2	55	66%

Example: voluntary cooperation by providers

- More than 130,000 requests/year by European States to major US providers
- Disclosure of subscriber or traffic data (ca. 60%)
- Providers decide whether or not to respond to lawful requests and whether to notify customers
- Provider policies/practices volatile
- Data protection concerns
- No disclosure by European providers
- No admissibility of data received in some States

► Clearer / more stable framework required

Crime and jurisdiction in cyberspace ► Issues and solutions under the Budapest Convention on Cybercrime

Solutions:

1. More efficient MLA [agreed by T-CY]
2. Guidance Note on Article 18 [approved by T-CY in February 2017]
3. Domestic rules on production orders (Article 18) [agreed by T-CY]
4. Cooperation with providers: practical measures [agreed by T-CY]
5. Protocol to Budapest Convention [negotiations started in Sep 2017]


www.coe.int/cybercrime