UNODC United Nations Office on Drugs and Crime | IAP International Association of Prosecutors | CTED Counter-Terrorism Committee Executive Directorate

Expert Group Meeting (EGM)
Lawful Access to Digital Data Across Borders
Development of the Practical Guide to Central Authorities (CAs), prosecutors and investigators for obtaining electronic evidence from foreign jurisdictions in counter-terrorism and related organized crime cross-border investigations
Vienna, Austria, 12-13 February 2018

Cooperation with multi-national service providers

Issues and options based on experience within the framework of the Budapest Convention on Cybercrime

Alexander Seger, Head of Cybercrime Division, Council of Europe
alexander.seger@coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

www.coe.int/cybercrime

1

Background: relevant provisions of the Budapest Convention

- By Feb 2018, 56 Parties + 14 Observer States (signatories + invited to accede)
- Definitions of "traffic data" (Article 1) and "subscriber information" (Article 18)
- Preservation powers
  - Articles 16 + 17 (domestic) and 29 + 30 (international)
  - Implementation assessed by T-CY in 2012 – 2015
- Production orders (Article 18),
  - including production of subscriber information regarding "service providers offering a service in its territory"
  - Guidance Note on Article 18 adopted by T-CY in February 2017
  - Article 18: partial legal solution to request subscriber info from providers abroad
- Search and seizure (Article 19), including extending a search to connected computer systems "in its territory"
- Transborder access to data (Article 32)
  - Guidance Note on Article 32 (Dec 2014): Service providers normally not a person able to consent
- See also: Guidelines on LEA/ISP cooperation (2008)
- European Court of Human Rights: K.U. v. Finland (2008)

2

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
  - When is a provider in a "territory" ▶ what connecting factors?
  - What determines territoriality: Location of data, device, person in possession or control, service?
  - 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

3

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

4

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%

5

Example: voluntary cooperation by providers

- More than 130,000 requests/year by Parties to major US providers in 2015 [more than 170,000 in 2017?]
- Disclosure of subscriber information (ca. 60%)
- Providers decide whether or not to respond to lawful requests and whether to notify customers
- Provider policies/practices volatile
- Data protection concerns (voluntary disclosure post May 2018 [GDPR] [see WHOIS]?)
- No disclosure by non-US providers
- No admissibility of data received in some States

► Clearer / more stable framework required

Solutions recommended by T-CY* Cloud Evidence Group in 2016:

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]

* T-CY = Cybercrime Convention Committee (Parties to the Budapest Convention)

7

Guidance Note on Article 18 Budapest Convention on production of subscriber information:

- Domestic production orders for subscriber information if a provider is in the territory of a Party even if data is stored in another jurisdiction (Article 18.1.a)
- Domestic production orders for subscriber information if a provider is NOT necessarily in the territory of a Party but is offering a service in the territory of the Party (Article 18.1.b)
- Connecting factors! "Real and substantive connection", "to be established"
- Enforcement?

8

Solution 5: Protocol to Budapest Convention

Proposals:

A. Provisions for more efficient MLA

B. Provisions for direct cooperation with providers in other jurisdictions

- Direct requests by LEA to a service provider abroad and disclosure by providers in specific situations and with conditions and safeguards
- Direct preservation requests to providers abroad
- Emergency procedures

C. Framework and safeguards for existing practices of transborder access to data

D. Data protection and other safeguards

- Terms of reference approved in June 2017
- Negotiations started in September 2017
- Scheduled to last until December 2019

9

10