

African Forum on Cybercrime, Addis Ababa, 16 – 18 October 2018

Workshop 7: Challenges of evidence in the cloud



EUROPEAN UNION

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE



Foreign &
Commonwealth
Office



Home Office



UNODC

United Nations Office on Drugs and Crime



INTERPOL



The Commonwealth

Evidence in the cloud: challenges, issues, solutions

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

www.coe.int/cybercrime

Crime and jurisdiction in cyberspace



Where is the data, where is the evidence? Where is the boundary for LEA powers?



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 ► Specific issues

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



Issue: Subscriber vs traffic vs content data

- **Subscriber information most often required in criminal investigations.**
- **Less privacy-sensitive than traffic or content data. Rules for access to subscriber information not harmonised.**
- **Subscriber information held by service providers and obtained through production orders. Lesser interference in rights than search and seizure.**



Issue: Loss of location

- In “loss of location” situations (unknown source of attack, servers in multiple or changing locations, live forensics, etc.) MLA not feasible ► principle of territoriality not always applicable
- Direct transborder access to data may be necessary
- What conditions and safeguards?
- Article 32b Budapest Convention limited ► Absence of international legal framework for lawful transborder access
- Unilateral solutions by governments / jungle ► risks to rights of individuals and state to state relations



Issue: Mutual legal assistance

- Mutual legal assistance remains a primary means to obtain electronic evidence for criminal justice purposes
- MLA needs to be made more efficient
- Often subscriber information or traffic data needed first to substantiate or address an MLA request
- MLA often not feasible to secure volatile evidence in unknown or multiple jurisdictions
- Loss of location: to whom to send an MLA request?

Direct cooperation with providers across jurisdictions

	Requests for data directly sent to Apple, Facebook, Google, Microsoft, Twitter and Oath in 2017		
<i>Parties and Observers (70 States)</i>	Received	Disclosure	%
Albania	27	14	53%
Belgium	2 521	2 301	91%
Cabo Verde	40	20	50%
Croatia	196	166	85%
France	29 400	18 466	63%
Germany	35 596	20 172	57%
Mauritius	2	0	0%
Morocco	30	18	59%
Nigeria	7	5	71%
Portugal	3 569	2 394	67%
Senegal	2	0	0%
Turkey	8 618	4 739	55%
United Kingdom	31 954	23 073	72%
Total (excluding USA)	170 680	109 093	64%



Direct cooperation with providers across jurisdictions

Example: Voluntary disclosure [of subscriber information] by service providers

Current practices:

- More than 170,000 requests/year by BC Parties/Observers to major US providers
- Disclosure of subscriber information (ca. 64%)
- Providers decide whether to respond to lawful requests and 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**



Issue: Data protection and other safeguards

- Data protection requirements normally met if powers to obtain data defined in domestic criminal procedure law and/or MLA agreements
- MLA not always feasible
- Increasing “asymmetric” disclosure of data transborder
 - From LEA to service provider ► Permitted in exceptional situations
 - From service provider to LEA ► Unclear legal basis
 - providers to assess lawfulness, legitimate interest
 - risk of being held liable
- = Clearer framework for private to public disclosure transborder required



Towards SOLUTIONS

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

- 1. More efficient MLA**
- 2. Guidance Note on Article 18**
- 3. Domestic rules on production orders (Article 18)**
- 4. Cooperation with providers: practical measures**
- 5. Protocol to Budapest Convention**



Solution 1: More efficient MLA

Example:

- ▶ Template: Mutual Legal Assistance Request for subscriber information (Art. 31 Budapest Convention)
- ▶ Template: Data Preservation Request (Articles 29 and 30 Budapest Convention)



Solution 2: Guidance Note on Production Orders

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)**
- **Foresee this in your domestic law**



Solution 3: Domestic rules on production orders

► Production orders of Article 18 needed in domestic law

Article 18 – Production order

- 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:**
 - a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and**
 - b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.**



Solution 3: Domestic rules on production orders

- **ECtHR: Case of Benedik vs. Slovenia**
- **T-CY Discussion paper**
- **Issues to addressed in domestic law:**
 - **Are providers allowed to retain subscriber information?**
 - **Is subscriber information related to dynamic IP addresses „traffic data“?**
 - **Are dynamic IP addresses always linked to a specific communication and thus protected by telecommunication secrecy?**



Solution 5: Protocol to the Budapest Convention on Cybercrime

A. Provisions for more efficient MLA

- Emergency MLA
- Joint investigations
- Video conferencing
- Language of requests
- Etc.

B. Provisions for direct cooperation with providers in other jurisdictions

C. Framework and safeguards for existing practices of extending searches transborder

D. Safeguards/data protection

Terms of reference approved in June 2017.

Negotiations: Sep 2017 – Dec 2019.



www.coe.int/cybercrime