Third Annual PILON Cybercrime Workshop
International Cooperation to Share Electronic Evidence and Combat Cybercrime
27 - 31 May 2019, Vanuatu

www.coe.int/cybercrime

1

Challenge: e-evidence on ANY crime

Cybercrime

- Offences against computer systems and data
- Offences by means of computer systems and data

+

Electronic evidence

- Any crime may involve evidence in electronic form on a computer system
- Needed in criminal proceedings
- No data, no evidence, no justice

2

Assessment of international cooperation under the Budapest Convention (2014)

International requests for data

Types of data requested:

1. **Subscriber information** (80+%?)
2. Traffic data
3. Content data

Underlying offences

1. **Fraud and other financial crimes**
2. **Violent and serious crime** (murder, assaualt, trafficking, child abuse etc.)
3. **Offences against computer systems**

3

Cybercrime and e-evidence: the problem of territory and jurisdiction

4

Crime and jurisdiction in cyberspace ► Solutions

Direct cooperation with service providers in other jurisdictions to obtain:

- **Subscriber information**
- **Any data in emergency situations**

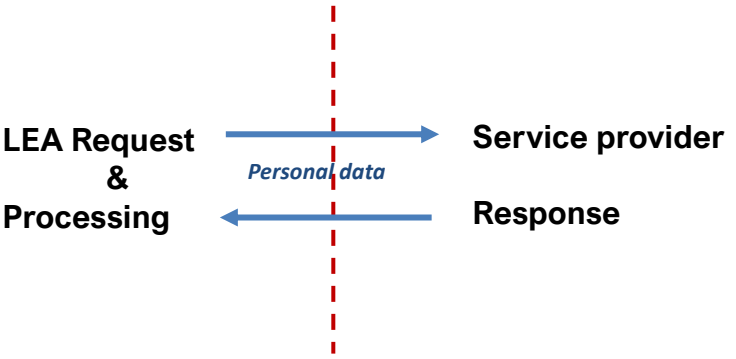
5

Current system of direct requests to providers

	Requests for data directly sent to Apple, Facebook, Google, Microsoft, Twitter and Oath in 2017		
Parties and Observers (70 States)	Received	Disclosure	%
Albania	27	14	53%
Australia	6 555	4 543	69%
Belgium	2 521	2 301	91%
Croatia	196	166	85%
France	29 400	18 466	63%
Germany	35 596	20 172	57%
Mauritius	2	0	0%
Morocco	30	18	59%
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%

6

Direct asymmetrical cooperation



Legal basis for processing? For transborder transfers?

7

Direct cooperation with providers: some issues

- ECtHR: Case of Benedik vs. Slovenia (T-CY Discussion paper)
- Issues to addressed in domestic law:
  - 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?
  - Data protection rules:
    - Is voluntary cooperation permitted?
    - Risks for providers?
- Admissible as evidence?
- Sovereignty/territoriality and reciprocity

8

Direct cooperation with providers: some issues

Direct cooperation with providers ► Practical measures (e.g. single points of contact, arrangements with providers) helpful

but:

► Clearer domestic and international legal basis needed

- ► Guidance Note Article 18 Budapest Convention
- ► Protocol to the Budapest Convention on Cybercrime

9

Solutions : 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

10

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

Negotiations:

Start - Sep 2017

End - 2020?

11