COUNCIL OF EUROPE CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Malaysian Communications and Multimedia Commission (MCMC)
Judicial and Legal Training Institute (ILKAP)
Council of Europe

Cybercrime training course

Jurisdiction and law enforcement in the clouds - challenges

ILKAP, Bandar Baru Bangi, Selangor , Malaysia (25-29 October 2010)

Alexander Seger
Council of Europe,
Strasbourg, France
Tel +33-3-9021-4506
alexander.seger@coe.int

1

1 Introduction

Live in a global borderless information/network society where our rights are protected by the constitutional nation state within geographical boundaries

Key issues in the online environment:
Data protection/privacy
Freedom of expression
Procedural safeguards/ due process
Security (CIA of data and systems)

Key questions:

how to ensure security while maintaining due process, freedom of expression and privacy in a global environment?
How to ensure security and privacy in the clouds?

2

2 Jurisdiction in the Budapest Convention

Jurisdiction is power of a sovereign state to regulate, to adjudicate and to enforce norms by which its legal subjects are bound

Budapest Convention on Cybercrime: territoriality and nationality principles

Article 22 – Jurisdiction

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a in its territory; or

b on board a ship flying the flag of that Party; or

c on board an aircraft registered under the laws of that Party; or

d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

Jurisdiction in the Budapest Convention

Article 22 – Jurisdiction cont'd

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1 [punishable one year or more], of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

3 Jurisdiction in the context of cloud computing

How to access data for criminal justice purposes that is physically stored on a server stored on a server on another territory. What jurisdiction?

„No server, no law“ or „no server, but service and therefore law“?

Is it permitted under domestic or international law to gather electronic evidence abroad (extraterritorial jurisdiction) without consent of that state?

What are the risks, problems?

Loss of location: where is the data anyway?

Jurisdiction in the context of cloud computing

What is cloud computing?

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Essential characteristics:	Service models:	Deployment models:
▪ On-demand self-service ▪ Broad network access ▪ Resource pooling ▪ Rapid elasticity ▪ Measured Service	▪ Cloud Software as a Service (SaaS) ▪ Cloud Platform as a Service (PaaS) ▪ Cloud Infrastructure as a Service (IaaS)	▪ Private cloud ▪ Community cloud ▪ Public cloud ▪ Hybrid cloud

4 Privacy and data protection issues

Data Protection in the clouds:

- Where is my data?
- What privacy/data protection data apply to data in the clouds?
- Same expectation of privacy if data is with cloud providers?
- What rules govern access by law enforcement/intelligence services.
- If data is stored on an individual computers system, citizens are in most countries protected against arbitrary searches by law enforcement. Does the same level of protection, the same procedural safeguards apply
  - to data backed up in a data centre of a cloud provider?
  - to data stored in a data centre in another country?
- Need to establish globally trusted privacy / data protection standards and systems

5 Law enforcement issues

- From a law enforcement/security perspective: need to trace the origin of an attack/offence, identify the offender to hold him/her accountable. Need access to traffic data, content data or other stored computer data, need subscriber information
- Normal procedure:
  - search, seizure, interception, preservation, production
  - safeguards in relation to computer data and systems in country of law enforcement investigation
  - international investigations: MLA + urgent measures for preservation
- Existing LEA approach “Data stored on a computer system”. With cloud computing: where is the computer system? Where is the data? How to get access?
- Existing instruments will remain valid. Full implementation of CCC more important than ever.

Legal and law enforcement issues

Data access "in the clouds"

1. Access to cloud data within the jurisdiction of law enforcement authorities:
   - Search, seizure and other procedural law provisions (Section 2 Budapest Convention)
2. Cloud data hosted abroad: Access with the assistance of law enforcement authorities of country hosting cloud servers
   - (Art 31 and other provisions of Chapter III Budapest Convention)

Legal and law enforcement issues

Data access "in the clouds"

3. Direct law enforcement access to cloud data abroad: Trans-border access by law enforcement to data stored abroad without involving cloud providers or authorities of the hosting country
   - Art 32b Budapest Convention with consent
   - Art 19 (2) Budapest Convention. Extending a search. Law enforcement lawfully search a computer and extend the search to a connected computer system (Art 19 (2) Budapest Convention). What if the connected system (the "cloud") is abroad? How can access be obtained?
   - If collected from abroad, can evidence be used in criminal proceedings without formal MLA?

Legal and law enforcement issues

About Article 32 of the Convention on Cybercrime

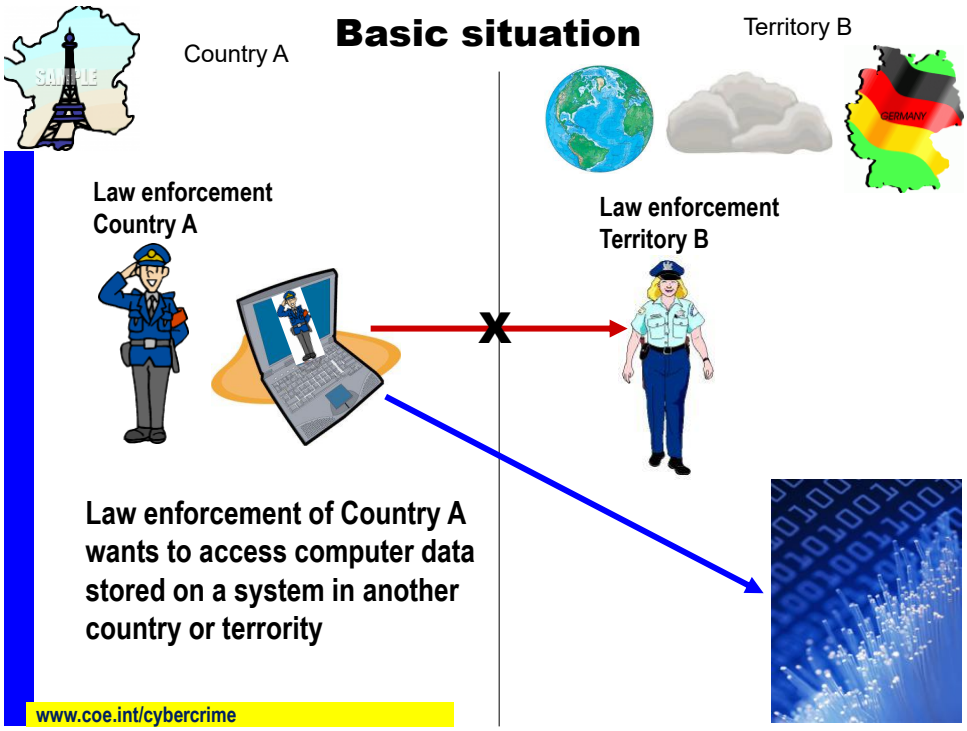
Legal and law enforcement issues

Article 32 – Trans-border access to stored computer data with consent or where publicly available

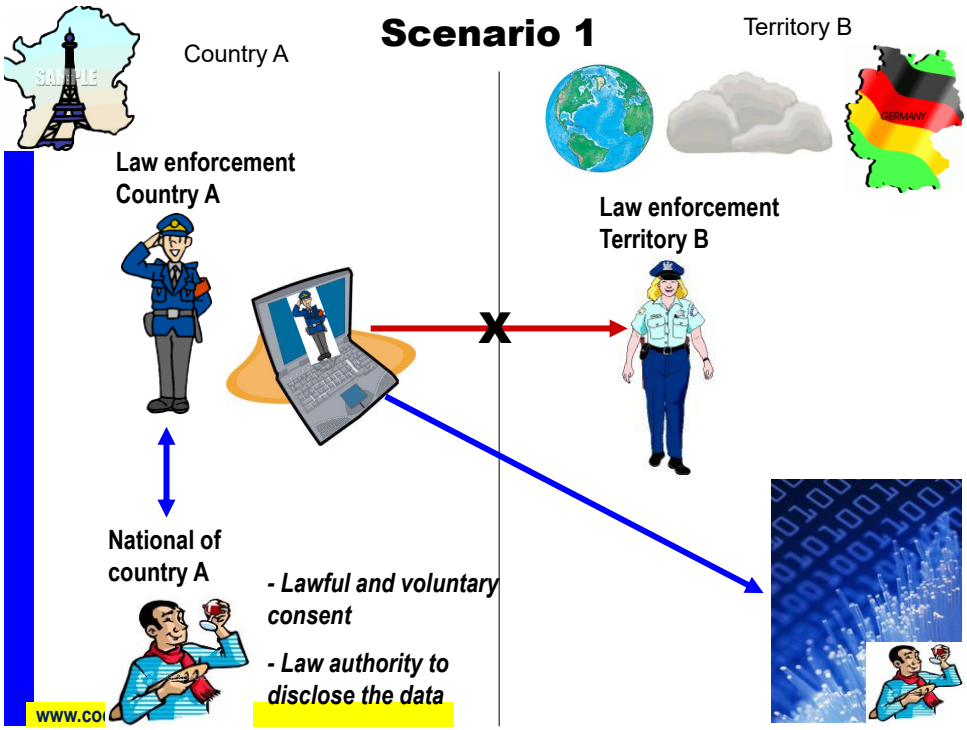
A Party may, <u>without the authorisation of another Party</u>:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

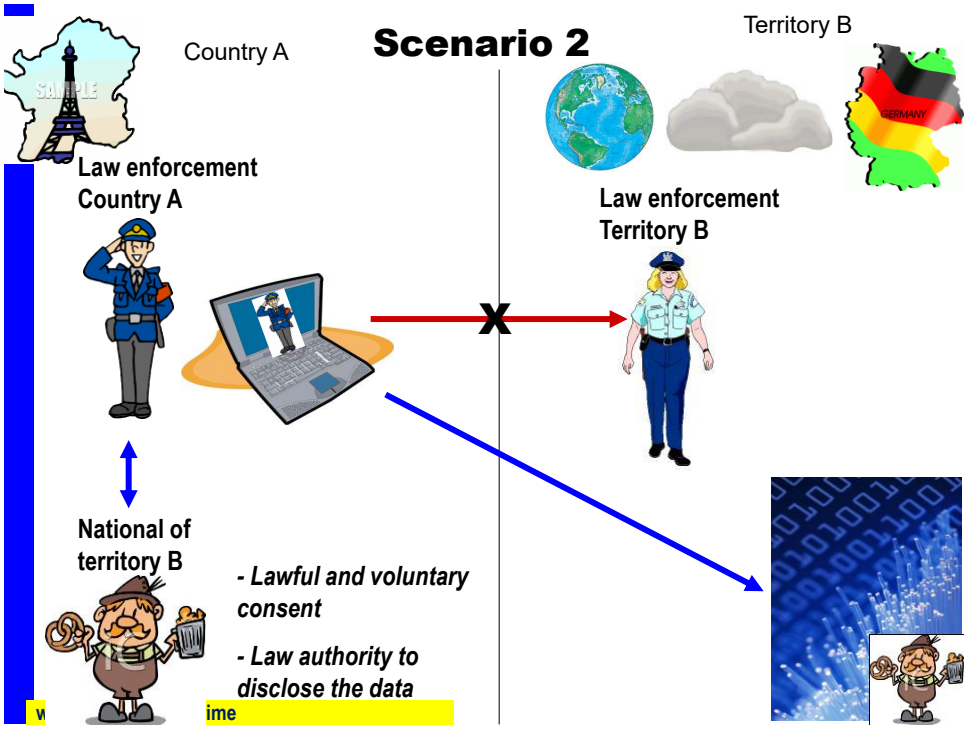
b access or receive, through a computer system in its territory, <u>stored computer data located in another Party</u>, if the Party obtains the <u>lawful and voluntary consent</u> of the person who has the <u>lawful authority to disclose the data</u> to the Party through that computer system.


Basic situation
Country A
Territory B
GERMANY
Law enforcement
Country A
Law enforcement
Territory B
X
Law enforcement of Country A wants to access computer data stored on a system in another country or terrority
www.coe.int/cybercrime

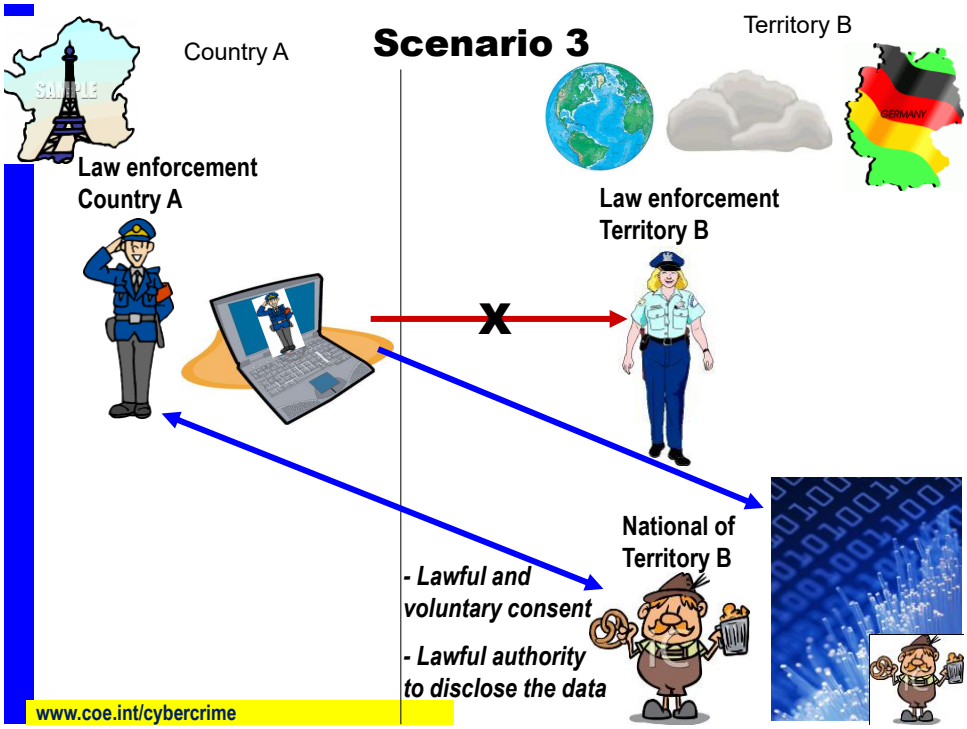
13


Scenario 1
Country A
Territory B
GERMANY
Law enforcement
Country A
Law enforcement
Territory B
X
National of
country A
- Lawful and voluntary consent
- Law authority to disclose the data

14


Scenario 2
Country A
Territory B
Law enforcement
Country A
Law enforcement
Territory B
X
National of
territory B
- Lawful and voluntary consent
- Law authority to disclose the data
ime

15


Scenario 3
Country A
Territory B
Law enforcement
Country A
Law enforcement
Territory B
X
National of
Territory B
- Lawful and voluntary consent
- Lawful authority to disclose the data
www.coe.int/cybercrime

16

Legal and law enforcement issues

Article 19 – Search and seizure of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:
a a computer system or part of it and computer data stored therein; and
b a computer-data storage medium in which computer data may be stored in its territory.

2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

Legal and law enforcement issues

Data access "in the clouds"

4. Access with the cooperation of ISPs/cloud providers

- Access by law enforcement to data of foreign natural or legal persons hosted (controlled, processed) on the territory of the law enforcement agency: what conditions?
- Law enforcement compelling cloud providers/ISPs to provide data hosted/controlled/processed abroad (traffic data, content data, coercive measures/interception): what conditions?

Cloud providers operating in multiple jurisdictions: what rules apply?

Need for guidance/international agreement?

Legal and law enforcement issues

Procedural safeguards (Art 15 Budapest Convention)

- Access to data to be based on law
- Confidentiality, integrity and availability of data and systems a basic right
- Judicial control over intrusive measures
- Conditions for access to data, approval by prosecutor or judge, for use of evidence

What safeguards against LE action if data stored abroad / in the clouds?

5 Conclusions: How to ensure security and privacy in the clouds?

1. Existing instruments make sense -> e.g. full implementation of Convention on Cybercrime
2. Enhance the efficiency of application of international cooperation provisions of the Convention on Cybercrime and others
3. Develop additional international standards on law enforcement access to data stored abroad / in the clouds
4. New concept for law enforcement access: from territoriality (physical location of data) to power of disposal (control of data) by a suspect?
5. Insist on procedural safeguards/due process / clear procedures for cooperation between cloud providers and law enforcement -> provide guidance to service/cloud providers
6. Establish globally trusted privacy / data protection standards and systems

Alexander.seger@coe.int