COUNCIL OF EUROPE CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Octopus Conference 2010 – Outlook session on security and privacy in the clouds

Law enforcement in the clouds - challenges

Strasbourg, 25 March 2010

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

1 Key question

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 question:

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 Information security issues in the clouds

- More security/less cybercrime because of professional protection measures of systems, software and data by cloud providers?
- More effective disaster recovery?
- Or clearer targets?
- How secure is cloud technology?
- Confidentiality/security on multi-tenant servers?
- What rules/regulations apply to cloud providers or data in the clouds?

3 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.

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

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?

   - Law enforcement compelling cloud providers/ISPs to provide data hosted/controlled/processed abroad (traffic data, content data, coercive measures/interception)?

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?

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
- Complexity and lack of harmonisation even within EU (data protection, data retention etc.)

Data protection/privacy: need for global trusted data protection/privacy policies

- Data protection/privacy a fundamental right
- condition for law enforcement cooperation
- condition for off-shoring
- Helps protect confidentiality, integrity and availability of data and systems

- CoE Convention on data protection Data (CETS 108)
- Protocol on supervisory authorities (CETS 181 of 2001)
- Rec (87) 15 regulating the use personal data in the police sector

- CETS 108 open for non-member States
- CETS 108 to be updated
- Recommendation on profiling in preparation
- Reforms of CoE + EU + OECD instruments -> need for cooperation

Interoperability of devices + need for authentication + cloud computing + IPv6

31st Meeting of data protection commissioners, Spain, Nov 2009 -> Proposal for international standards on privacy and personal data protection

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

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

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. Insist on procedural safeguards/due process / clear procedures for cooperation between cloud providers and law enforcement -> provide guidance to service/cloud providers
5. Establish globally trusted privacy / data protection standards and systems
6. Cloud provider that cannot guarantee data protection/privacy standards and procedural safeguards will have a competitive disadvantage

Alexander.seger@coe.int