Liabilities of ISPs
Rsponsabilities of Regulators

Regional Event Chisinau

September 2017

Study: purpose

- Understand the legislative framework in EAPIII countries regarding:
  - Access to data for LEA (interception, retention)
  - General Liability of ISPs
  - Safeguards (balancing privacy and acsess obligations, transparency)
  - Data retention
  - Role of Regulators
  - (Public-Private) Cooperation

Program

- Overview and recommendations in each area:
  - Access to data for LEA (interception, retention)
  - General Liability of ISPs
  - Safeguards (balancing privacy and acsess obligations, transparency)
  - Data retention
  - Role of Regulators
  - (Public-Private) Cooperation

Law enforcement online

ACCESS TO DATA

Legal framework: outline

- Budapest Convention on Cybercrime
  - Section 2: provides required powers (artt. 16 and further)
  - Article 15 (!): human rights and liberties.
- Human rights:
  - European Convention on Human Rights (CoE)
  - Universal Declaration of Human Rights 1948 (UN)
  - International Covenant on Civil and Political Rights (UN)

Legal framework: continued

- Member states will have to create balanced regimes due to right to Privacy
- Safeguards/Importance of independent oversight:
  - ECHR caselaw
  - Balancing act:
    - "Necessary in a democratic society"
    - "Proportionality and subsidiarity"
  - Transparency

Case Law

- Van der Velden vs. The Netherlands:
  - New technologies (DNA database) and right to Privacy
  - Crime Prevention (Preventive entry) allowed as necessary and
  - DNA swab of criminals is proportional if not discriminatory

Sakharov

- Russian SORM interception:
  - Communications surveillance is permitted for a broad range of criminal offenses and authorities have "an almost unlimited degree of discretion" in the matter;
  - Surveillance is not limited to those suspected of having committed offenses;
  - Criteria for beginning, ceasing and scope of the surveillance are not clearly defined;

Sakharov II

- Robust oversight mechanisms and effective remedies were lacking, mainly:
  - Logging or recording of the interceptions is prohibited by Russian law;
  - Supervision of interception by judges and prosecutors is limited, does not include checks for necessity and justification, and is not open to public scrutiny;
  - The absence of a requirement to notify the subject when surveillance had ceased undermines the effectiveness of any available remedies

Case law

- Szabo & Vissy:
  - Interception with independent oversight?
  - Positive obligation for effective prosecution.

Case Law

- Szabo & Vissy (Continued):

  "The Court is not convinced that the Hungarian legislation on 'section 7/E(3) surveillance' provides **safeguards** sufficiently **precise**, **effective** and **comprehensive** on the ordering, **execution and** potential **redressing** of such measures. Given that the scope of the **measures could include virtually anyone**, that **the ordering is taking place entirely within the realm of the executive and without an assessment of strict necessity**, that **new technologies enable the Government to intercept masses of data easily concerning even persons outside the original range of operation**, and given the **absence of any effective remedial measures**, let alone judicial ones, the Court concludes that there has been a violation of Article 8 of the Convention."

Case Law

- Transparency:
  - Youth Initiative for Human Rights vs. Serbia: be transparent about numbers of interceptions in criminal cases.
  - Orange Slovensko, A. S. v. Slovakia: Pre-installation of Wire tap Equipment can be lawful (if..)

Data Retention

- Digital Rights Ireland:
  - ECJ applying ECHR by way of EU Charter of Human rights.
  - Traffic data retention (directive)
  - Again: safeguards, defined purpose of retention
  - Retention period based on objective criteria!

EAP III

- Findings:
  - Preservation and Production in individual case
  - Retention
  - Interception

Findings – Preservation orders

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Rules in Place	Yes	No information provided	Yes	No information provided	No	No
Legislative Basis	Yes	No information provided	Yes	No information provided	Yes	No
Enforcement Authority	National Security Agency	No information provided	State Security Committee, Operative and Analytical Centre	No information provided	Prosecutor's Office, Police	Prosecutor's Office
Access to Preserved Data	Court Order	No information Provided	Prosecutor's Order	No information provided	Court Order	Police, Security Service or Antimonopoly Committee Order

Findings - Interception

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Basis for Legal Interception	Law	No information provided	Law	No information provided	Law	Law
Requirement to Provide Ability	License Condition	No information provided	Law	No Information Provided	Law	Law

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Legal Interception Practical Approach	Black Box	No information provided	Black Box	No information provided	No information provided	No information provided
Cost Borne By	ISP	No information provided	ISP and Law Enforcement	No Information Provided	ISP	ISP

Recommendations

- Keep in mind the cost aspect: this benefits cooperation.
- Keep in mind the required transparency (!)

A good basis for cooperation?

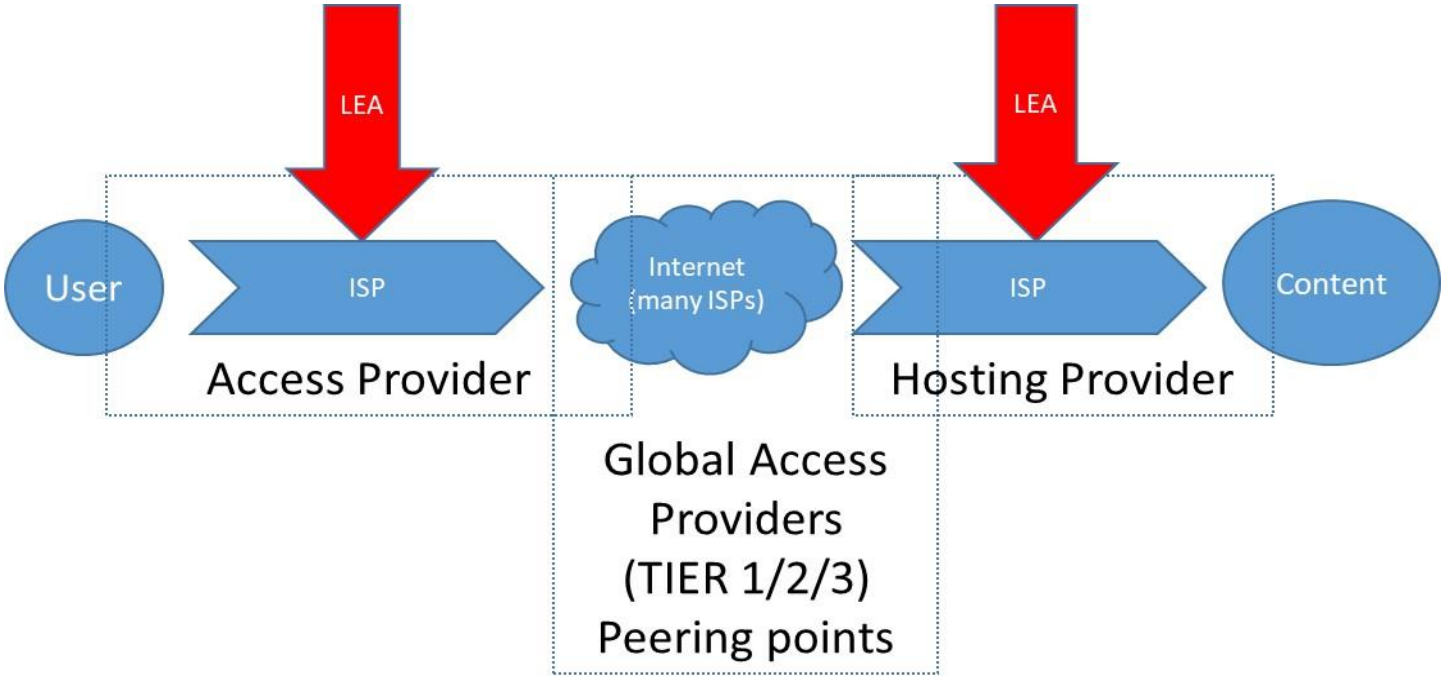
LIABILITY FRAMEWORK FOR ISPS

ISP liability

- Classic liabilities towards government:
  - Access to data
  - License conditions
  - Public interest related (privacy security)
- Other issue:
  - Liability for content transmitted

Liabilities & ISPs

- ISP roles and Liabilities



Framework

- Some Liability is assumed
- However:

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
ISP Liability for user content	None – based on Telecoms law and Net Neutrality requirements.	No information provided	Only upon notice by competent authority.	No specific regulation.	No specific regulation. No	None – based on Telecommunications law

Issue

- Not sure if this is a "horizontal" analysis.
- Can ISPs see liablities brought against them in practise?
- Can specific telecommunications **obligations** be leveraged against anyone as a **defence**?

EU framework

- Differing roles:
  - Access: only subject to blocking order if requsted by court/authority.
  - Hosting: may be liable if "actual knowledge"of illegal content exists, and provider does not act "expeditiously".
  - No obligation to monitor.

Role differentiation

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
ISP role division	NO	No information provided	Partly (reporting regime)	No.	No.	No.

Issue

- Could role of ISPs be broadened if more responsibility was given to them?
- More cooperation if more responsibility?

Monitoring and reporting

- None (or limited) monitoring obligations
- No reporting obligations.
  - One exception: owners of sites in Belarus.
- No issues here…

Opportunity

- Reporting obligations can be considered. Could these be leveraged?
  - What if reports arrive at ISP?
    - Child abuse
    - Network abuse
    - Security issues at end users

Recommendations

Short summary:

- Consider broader responsibility.
- But keep in mind this requires a very carefully balanced regime.
- Independent oversight.

Adequate redress for all parties, includeing end users and industry?

SAFEGUARDS

Safeguards

- What to safeguard?
  - Privacy
  - Subscriber information
- How to safeguard?
  - Obligation for ISPs
  - Enforcement regime

Findings

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Protect Secrecy of Communication	Yes	No information provided	Yes	Yes	Yes	Yes
Protect Subscriber Identity	Yes	No information provided	Yes	Yes	Yes	Yes

Legal intercept: basis

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Order Required for Interception	Court Order	No information provided	Prosecutor Order	No information provided	Prosecutor Order	Court Order

Oversight and enforcement?

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Authority Responsible for Oversight	Regulator, Law Enforcement, Data Protection	No information provided	Inspectorate for Telecommunications, Operative and Analytical Centre	Data Protection Authority, National Commission on Communications	Communications Regulator	Not Defined
Enforcement Measures	Administrative Sanctions	No information provided	Administrative Sanctions	Administrative Sanctions	Civil Sanctions	Administrative and Criminal Sanctions

Recommendations

- More independence of oversight.

Traffic data as evidence

DATA RETENTION REGIMES

Findings

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Data retention obligation (basis)	Regulator (PSRC) – policy and MoU (Voluntary)	No information provided	Presidential decrees and ministerial decrees	No information provided	Law	Law
Retention period voice/phone	2 Years	No information provided	5 years	No information provided	180/90 days (traffic/decryption keys)	3 years
Retention Period data	Voluntary (MoU)	No information provided	5 years	No information provided	180/90 days	3 years
Definition of traffic data (internet)	Yes	No information provided	Not available	No information provided	Yes	Not available

Recommendations

- Observe clear legal basis
  - Keep in mind the ECHR/ECJ requirements on the regime!
- Oversight.

Roles of Regulators

REGULATORY AUTHORITIES

Roles

- Not for CoE to decide on precise role division
- Some requirements as to independence frome executive (ECHR/ECJ)
- EU Best Practise: independent regulator

Findings

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Seperate regulator	Yes (PSRC)	No information	No	Yes (GNCC)	Yes (Ancreti)	Yes (NCCIR)
Access to data	Yes	No information	LEA & Operational Center	No Information	Yes	No
Interception of content data	Yes (License condition)	No information	KGB& Operational Center	No Information	Yes (Also GPO & Police)	No
Privacy and consumer rights	Yes (consumer protection)	No information	Ministry of Communications, Oprational Center	Yes	Yes	Yes
Cyber security strategy	Yes	No information	Yes	Yes	No information	No

Recommendations

- Independence of regulator
- Cooperation is preferable
- Oversight on access to data/data retention: not dome by LEA! Independence from executive.

Several types of cooperation

COOPERATION

Overall

- Overall regime (MoU?)
- Cooperation on:
  - Takedown of content?
  - Fraud/Financial damage?
  - Threat intelligence?
  - Awareness/Training

Overall regime

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Cooperation Agreements	No	No information provided	Yes	No information provided	No information provided	No

Takedown of content

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Illegal Content Takedown Requirement	Court Order	No information provided	No information provided	Court Order	Court Order	Court Order
Fast Takedown Possible	Yes	No information provided	Yes	No Information Provided	No Information Provided	Partial

Financial frauds

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Obligation to Prevent Fraud or Financial Damage	No obligation	No information provided	In some cases	In some cases	No information provided	No information provided

Threat intelligence

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Information Sharing	Informal	No information provided	No information provided	Informal	No information provided	No information provided
Information sharing platform	Informal CERT	No information provided	National CERT	No information provided	No information provided	No information provided
Feedback provided	No	No information provided	Yes	No information provided	No information provided	No information provided

Training and awareness

- To be provided DOR

Overall

OVERALL CONCLUSIONS

Overall conclusions

- Better legal basis and better oversight required in some cases
- Role of ISPs and responsibilities regarding content could be explored
- Independence of regulator
- More scope for Cooperation in several areas

Questions

- ?
- Hein Dries
- hein@vigilo.nl
- +31 71 7113243