European Parliament LIBE Committee Hearing
Cross-Border Access to Electronic Evidence

27th November 2018, Brussels, European Parliament

Dr. Maximilian Schubert LL.M
Vice-President, Chair Cybersecurity Committee, EuroISPA
General Secretary, ISPA Austria
Agenda

• About EuroISPA

• E-Evidence Proposal: A significant shift in cross-border access to electronic evidence

• Legal Uncertainty for Service Providers

• Notification Procedures

• Further Concerns

• Towards a European Solution
About EuroISPA
EuroISPA: The Voice of ISPs in Europe

• Established in 1997
• The world’s largest association of Internet Service Providers (ISPs), representing over 2,500 ISPs across the EU and EFTA countries
• Representing many SME-ISPs
• Reflects the views of ISPs of all sizes from across its member base
E-Evidence Proposal: A significant shift in cross-border access to electronic evidence
Law Enforcement data requests to an ISP
Law Enforcement data requests to an ISP in a third country

Current MLAT Procedure
Law Enforcement data requests to an ISP in a third country

Current MLAT Procedure
Law Enforcement data requests to an ISP in another EU Member State

Current MLAT Procedure
Law Enforcement data requests to an ISP in another EU Member State
Law Enforcement data requests to an ISP in another EU Member State

Transition from MLAT to e-evidence system will lead to substantial changes in respect to the exchange of data.
Lack of Integrated *Procedural* Safeguards

- **Judicial review**: according to CJEU jurisprudence, access to retained data by national authorities should be subject to *prior review* by a court or independent administrative authority (*Tele2*, point 120)

- **Necessity and proportionality assurances**: sufficient information should be provided to service providers to have the *option* to raise concerns over Production Orders

- **A certain degree of authority involvement**: greater safeguards further to those of the issuing authority—either of the country of the affect data subject or the executing country
Lack of Integrated **Material** Safeguards

- **Criminal offence threshold**: significant disparity across Member States for crimes entailing a three-years sentence
- **A list of prescribed offences** such as in the EIO is still very broad, providing little further clarity
- **Necessity and proportionality tests** should be bolstered
- **Threshold of proof**: the more intrusive the data category requested, the higher the threshold of proof to request access to the data should be
Legal Uncertainty for Service Providers
Legal Uncertainty for Service Providers

The issue of dual criminality is key to guarantee legal certainty for Internet Service Providers

Insufficient authentication of Order Certificates

- ISPs unable to verify the authenticity of each national judicial authorities’ stamp and signature
- Conditions for security and integrity in executing a Production Order (data transfer)
- Reservations against downgrading to existing information exchange routines to e.g. fax transmissions
- Single Points of Contact (SPOC) on side of LEA would improve communication process
Legal Uncertainty for Service Providers

The issue of dual criminality is absolutely essential to guarantee legal certainty for Internet Service Providers.

Insufficient authentication of Order Certificates

- The need to verify the authenticity of orders.
- The importance of security and integrity.
- The requirement of downgrading information exchange routines.

EurISPA
Austrian Example for Safe Data Transfer between LEAs and ISPs: ‘DLS’
Notification Procedures
Notification of User and Judicial Authority

- Notification to the **user**: notification of request to access data to be obligation of issuing authority
  - CJEU jurisprudence: transparency, not confidentiality, should be the rule
- Notification to **judicial authorities**: notification system to the respective judicial authority alongside Production Orders
  - Notification to be undertaken by the issuing authority: greater legal clarity for service providers with judicial authorities’ awareness of Order
Notification of Judicial Authority

Ministry State A

Judicial Authority State A

LEA State A

ISP State B

Notification of Judicial Authority

Data handed over

Ministry State B

Judicial Authority

EPOC / EPOC-PR - Request for data
Further Concerns
E-Evidence Proposal: Further Concerns

Lack of an MSME exemption
• SME exemptions should be included to offset the considerable administrative, legal and financial burden incurred by the proposed e-evidence mechanism

Fragmentation of data categorisation
• Coherence in data categories across different legislation

Coherence with international standards
• Data transfers to LEAs in third-countries should be in line with international standards (i.e. Budapest Convention and EU-US MLAT)
E-Evidence Proposal: Further Concerns

Timeframes are not feasible
• Execution of a Production Order should be undertaken “expeditiously” rather than under a prescriptive deadline

Sanctions mimicking the GDPR are disproportionate
• Such draconian measures would create an environment of disclosure without consideration
E-Evidence Proposal: Further Concerns

Transparency
• Proposal lacks an enforcement mechanism securing the provision of statistics on issued orders
• ISPs should be free to publish voluntary transparency reports

Protection of encrypted data
• Clarification needed that ISPs are not required to decrypt data
• Transfer of encrypted data bears risk that more data is handed over than necessary

Danger of weakening the high level of trust and security
Maintaining an EU-wide high level of transparency and security
Towards a European Solution

• EuroISPA has longstanding experience in cooperating with judicial authorities

For a practical and secure e-evidence mechanism:

• Maintain the high level of safeguards
• Greater legal certainty
• Security and integrity in data request and transmission
• A solution which works for all players in the European Internet ecosystem
Thank You!

EuroISPA
European Internet Services Providers Association
Rue de la Loi 38- 1000 Brussels
T: +32 (0)2 550 41 22
www.euroispa.org

EU Transparency Register No. 54437813115-56

Dr. Maximilian Schubert, General Secretary
ISPA - Internet Service Providers Austria
Währinger Straße 3/18 - 1090 Vienna
T: +43 1 409 55 76

Email maximilian.schubert@ispa.at
Web www.ispa.at

EU Transparency Register No. 56028372438-43
BACKUP
Description of Austrian DLS Model I

• DLS resembles a blind mailbox system
• DLS provides a web-client
• DLS ensures traceability of all requests and responses, augmented with statistical data
• DLS acts as Certificate Authority
Description of Austrian DLS Model II

Independent layers of security
• Checks-and-Balances-Architecture
• Transport layer encryption
• Client controlled data encryption and signing
• Access Control

Independent methods of verification
• Request form verifiable independently of DLS
• Transmitted data verifiable via DLS (-Client)

CSV... Comma separated value (Technology neutral standard)
Description of Austrian DLS Model III

Advantages
• Not bound to particular technical requirements or products (Neither for providers nor for authorities)
• Can be utilized within all common databases
• Nearly no costs for implementation

Requirements
• Syntax and semantic of the CSV-file for data transmission must be defined
• All stakeholder have to agree on the interface