

Law enforcement - service provider cooperation in the investigation of cybercrime

Alexander Seger
Economic Crime Division, Council of Europe
Strasbourg, France
alexander.seger@coe.int

www.coe.int/cybercrime

1

Why law enforcement authorities (LEA) / Internet service provider (ISP) cooperation is necessary:

- Information society dependend on ICT - vulnerable to cybercrime - Need to enhance security of ICT
- LEA and ISP play crucial role in a secure Internet
- LEA investigations often not possible without ISP cooperation
- Ensure efficient work of LEA
- Protect ability of ISP to provide services
- Ensure due process
- Protect rights of users
- How to enhance, how to structure cooperation?
- Guidelines

To be taken into account:

- **Diverse set of stakeholders**
- **Make use of good practices**
- **Security – human rights: a question of balance?**
- **Applicability global**
- **Supplement/not replace legislation**
- **To be based on common legal standards**

3

3

Common legal standard: Convention on Cybercrime

- **Substantive criminal law: criminalising conduct**
- **Procedural measures: expedited preservation, production order, search and seizure, interception of data**
- **International cooperation**

- **Global trend towards strengthening of cybercrime legislation**
- **CCC common standard: used in 100+ countries world wide (but 13 EU M/S still need to ratify the Convention)**
- **Common issue: LEA-ISP cooperation**

4

4

Law enforcement authorities (LEA) / Internet service provider (ISP) cooperation: developing guidelines

- **Council of Europe Project on Cybercrime**
- **Working group Oct 2007 to March 2008**
- **Background study**

5

5

Law enforcement authorities (LEA) / Internet service provider (ISP) cooperation: developing guidelines

Background study/good practices:

- **Formal and informal relationships**
- **German E-Commerce Association/BKA agreement Nov 2007**
- **MoUs Microsoft – LEA in different countries**
- **eBay ELBA (electronic LE request processing system)**
- **AFA ISP-LEA training**
- **ECO SpotSpam**
- **Digital Phishnet**
- **French Signal Spam project**
- **MS CETS**
- **ISP training LEA**

6

6

Law enforcement authorities (LEA) / Internet service provider (ISP) cooperation: developing guidelines

Background study/bad practices:

- One request for multiple accounts
- Multiple requests that are LEA fishing expeditions
- LEA request for content without appropriate legal procedure
- Unclear, unspecific requests
- Requests sent to wrong person or provider
- ISP refuse to provide information without clear reason
- LEA receive incomplete responses/information
- Preservation requests not followed by production order

7

7

Law enforcement authorities (LEA) / Internet service provider (ISP) cooperation: developing guidelines

Background study/controversies:

- Small versus large ISPs
- Cost
- ISP liability
- ISP reporting requirement

8

8

Guidelines for the cooperation between law enforcement and internet service providers against cybercrime

Adopted at the global Conference on Cooperation against Cybercrime (Council of Europe, Strasbourg, 1-2 April 2008):

- **Common measures (including protection of rights and freedoms)**
- **Measures to be taken by law enforcement**
- **Measures to be taken by service providers**

9

9

Common guidelines for LEA and ISP:

- **Develop a culture of cooperation**
- **Develop written procedures for cooperation with each other**
- **Cooperate for the protection of rights and freedoms of individuals**
- **Respect each others roles, rights and limitations**
- **Mindful of cost of cooperation**
- **Etc**

10

Measures to be taken by law enforcement

- **Broad and strategic cooperation with ISP**
- **Procedures for legally binding requests**
- **Designated and trained personnel for cooperation**
- **Verification of source of requests**
- **Standard request format**
- **Specificity and accuracy of requests**
- **Follow preservation orders with production/disclosure orders**
- **Criminal compliance programme**
- **International requests: 24/7 network and formal mutual legal assistance**

11

11

Measures to be taken by ISPs

- **Report criminal incidents**
- **Assist LEA with training and other support**
- **Procedures for responding to requests**
- **Designated and trained personnel for cooperation**
- **Emergency assistance outside business hours**
- **Criminal compliance programme**
- **Verification of source of requests**
- **Standard response format**
- **Explanation for information not provided**
- **Coordination among ISP**

12

12

Important:

- **Guidelines, not binding**
- **Not substitute for procedural law and other formal regulations**
- **Based on good practices already available**
- **Help LEA and ISP in any country to structure their cooperation**

13

13

The way ahead:

- **Guidelines taken up by countries by organisations**
- **Specifically: Where to go from here?**
- **Question of process: Support process towards LEA-ISP cooperation**
- **Draft EU recommendations to support momentum in EU M/S**

Council of Europe

- **EuroDIG (Strasbourg, 20-21 October 2008)**
- **Internet Governance Forum (Hyderabad, 3-6 December 2008)**
- **Octopus Global Conference 2009 (Strasbourg, 10-11 March)**
- **Project on Cybercrime (Phase 2) (March 2009 – June 2011)**

14

14



Thank you.

Alexander.seger@coe.int

