COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/TCY

Strasbourg, 21 May 2018 T-CY (2018)16

Cybercrime Convention Committee (T-CY)

Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime

Discussion Guide for consultations with civil society, data protection authorities and industry

Octopus Conference, 11-13 July 2018

Council of Europe, Strasbourg, France

Participation in the consultations

Consultations on the ongoing preparation of a 2nd Additional Protocol to the Budapest Convention will be held within the framework of the Octopus Conference on Cybercrime from 11 to 13 July 2018, and specifically on Thursday, 12 July.

They are to permit an exchange of views between representatives of the Cybercrime Convention Committee and:

- **Civil society organisations and academia**
- **Data protection experts**
- **Industry (service providers and associations)**

Interested stakeholders are invited to **register** for the Octopus Conference between **1 May and 10 June 2018.** Conference space is limited. Interested stakeholders may also send **written comments** on the questions raised in this guide by **25 June 2018** to nina.lichtner@coe.int.

The Terms of Reference for the preparation of a draft 2nd Additional Protocol provide a general framework of elements for consideration. The final provisions of the Protocol are not set and negotiations are at a very preliminary stage.

Agenda

Preparation of the Protocol

- Overview, procedure and current state
- Further consultations with civil society, data protection and industry organisations

Context: Rationale for the Protocol – Recap and recent developments

- Setting the scene
- Related international developments: EU e-evidence proposals, US CLOUD ACT

Provisions for more efficient mutual legal assistance

Information and exchange of views on:

- Emergency mutual legal assistance
- Expediting mutual legal assistance for subscriber information
- Language of requests
- Audio/video hearings of witnesses, victims and experts
- Joint investigations and joint investigation teams

Direct cooperation with providers across jurisdictions

Discussion on preliminary options to address challenges:

- Voluntary cooperation models
- Production orders
- Data protection and other conditions and safeguards
- Implications on concepts of jurisdiction

Lawful access to data in the cloud

Discussion on preliminary options to address challenges:

- Understanding jurisdiction: Connecting factors
- Article 32 Budapest Convention
- Options to delimit practices
- Conditions and safeguards

1 Background

The evolution of information and communication technologies – while bringing unprecedented opportunities for mankind – also raises challenges, including for criminal justice and thus for the rule of law in cyberspace. While cybercrime and other offences entailing electronic evidence on computer systems are thriving and while such evidence is increasingly stored on servers in foreign, multiple, shifting or unknown jurisdictions, that is, in the cloud, the powers of law enforcement are generally limited by territorial boundaries.

The Parties to the Budapest Convention – represented in the Cybercrime Convention Committee – have been searching for solutions for some time, that is, from 2012 to 2014 through a working group on transborder access to data and from 2015 to 2017 through the Cloud Evidence Group.

Further to the results of the Cloud Evidence Group, the T-CY adopted the following Recommendations:

1. Enhancing the effectiveness of the mutual legal assistance process by giving follow up to earlier Recommendations adopted by the T-CY in December 2014.
2. A Guidance Note on Article 18 Budapest Convention on production orders with respect to subscriber information.
3. Full implementation of Article 18 by Parties in their domestic law.
4. Practical measures to enhance cooperation with service providers.
5. Negotiation of a 2nd Additional Protocol to the Budapest Convention on enhanced international cooperation.

In June 2017, the T-CY agreed on the Terms of Reference for the preparation of the Protocol during the period September 2017 and December 2019. The following elements are to be considered:

A. Provisions on more efficient mutual legal assistance (such as expedited MLA for subscriber information, international production orders, joint investigations, emergency procedures etc.).
B. Provisions on direct cooperation with providers in other jurisdictions with regard to requests for subscriber information, preservation requests, and emergency requests.
C. Clearer framework and stronger safeguards for existing practices on transborder access to data.
D. Safeguards, including data protection requirements.

The Terms of Reference for the preparation of a draft 2nd Additional Protocol provide a general framework of elements for consideration. However, the final provisions of the Protocol are not set; the feasibility of each of the issues, including those discussed today and other issues that may arise, will need to be determined during the negotiation of the Protocol.

The T-CY agreed to extend regular plenary meetings for negotiation of the Protocol and to establish a "Protocol Drafting Group" to work on text in between plenary sessions.

Protocol Drafting Group and subgroup meetings were held in September 2017, February 2018, April 2018 and May 2018 while a Protocol Drafting Plenary was held in November 2017 and a further one is scheduled for July 2018.

These meetings discussed concepts for provisions to be developed and worked on preliminary text of provisions aimed at more efficient mutual legal assistance (language of requests, audio/video hearings, emergency MLA). However, by May 2018, drafts had not sufficiently matured to warrant consultations with other stakeholders.

Before proceeding with the preparation of more complex provisions (such as direct cooperation with providers, framework for practices of transborder access, rule of law and data protection safeguards), the T-CY wishes to engage in a first round of consultations with civil society, data protection and industry organisations.

2 Objective of the consultations

The Cybercrime Convention Committee (T-CY) wishes to consult civil society, data protection organisations and industry during the drafting process in order to seek their views and benefit from their experience.

The Octopus Conference from 11 to 13 July 2018 will be an opportunity for such consultations. A one-day workshop will be dedicated to this on Thursday, 12 July.[1] Further meetings will be organised as draft concepts and text become available.

3 Issues for discussion

3.1 Context: Rationale for the Protocol – Recap and recent developments

This aim of this session is to recapitulate and reconfirm the rationale for the preparation of a 2nd additional Protocol to the Budapest Convention. Participants are also invited to discuss recent developments and their possible implications on the work on the Protocol.

▶ **Setting the scene**

- The growing global reach of the Budapest Convention and the need to take into account the laws, requirements and practices of all Parties.

- Challenges of criminal justice access to data in the cloud.

- Criminal justice scope of the Protocol: criminal investigations and proceedings related to cybercrime and electronic evidence (Articles 14 and 25.1 Budapest Convention).

- Specific issues to be to be considered in the development of the Protocol:
  - the need to differentiate between subscriber, traffic and content data in terms of requirements and thresholds for access to data needed in specific criminal investigations;
  - the question of expedited disclosure of subscriber data;
  - situations of loss of (knowledge of) location of data, or where the location of data is known to be in the territory of another State;
  - the fact that States increasingly resort to unilateral transborder access to data without clear international rules and where mutual legal assistance may not be feasible;
  - the challenges to mutual legal assistance for securing and obtaining volatile electronic evidence from another State, and ways to improve mutual legal assistance;
  - the current regime of voluntary disclosure of data by US-providers, limits on disclosure by providers located in other States, and ways to facilitate direct contact between law enforcement and providers;

[1] A further workshop on access to WHOIS data will take place in the morning of 13 July.

- the question of expedited disclosure of data in emergency situations;
- the need for safeguards and conditions, to include data protection, that ensure the adequate protection of human rights and liberties as applied to Parties of many different legal systems and cultures.

▶ **Relevant international developments**

– Location of data or location of data controller or location of person in possession or control:
  - Territoriality and the question of data localisation requirements;
  - Representatives of data controllers or processors (Article 27 GDPR), representatives of digital service provider offering a service within the EU (recital 65 and Article 18 NIS Directive);
– US CLOUD Act;
– European Union proposals on E-Evidence[2].

a Question: What are the implications of these developments for work on the Protocol?

3.2 Provisions for more efficient mutual legal assistance

Rendering mutual legal assistance on cybercrime and e-evidence more efficient is a priority of the Parties to the Budapest Convention. Therefore, the initial phase of the drafting process has been focusing on provisions related to MLA. The aim of this session is to brief participants on progress made in this respect.

▶ **Introduction: T-CY Recommendations 2014 and follow up given by Parties**

▶ **Information and exchange of views on:**

– Emergency mutual legal assistance;
– Language of requests;
– Audio/video hearings;
– Joint investigation teams.

b Question: Would civil society, data protection or industry organisations have any comments on such proposals?

3.3 Direct cooperation with providers across jurisdictions

Parties to the Budapest Convention – other than the USA – are sending more than 150,000 requests per year directly to major US service providers who voluntarily disclose subscriber information in about 60% of the cases to foreign criminal justice authorities. US providers may also voluntarily disclose content data in emergency situations via a US governmental entity. Policies, practices and response rates by providers to countries vary and they raise some concerns. At the same time, providers of most other countries are not able to voluntarily disclose data upon direct request to foreign authorities. Parties are exploring initial proposals for inclusion in the Protocol including:

[2] Comprising proposals for a:
- Regulation on production orders https://ec.europa.eu/info/sites/info/files/placeholder.pdf
- Directive on legal representative https://ec.europa.eu/info/sites/info/files/placeholder_0.pdf

(a) a clearer legal framework amongst Parties for the voluntary disclosure of subscriber information – and in emergency situations also other data – by providers;
(b) options for the mandatory disclosure of subscriber information;
(c) direct preservation requests to providers.

This session is to discuss the feasibility of these options and their compatibility with data protection requirements.

► **Voluntary disclosure [of subscriber information] by service providers**

- Brief review of current practices.[3]

- The scope and limitations of Article 18 Budapest Convention (see Guidance Note on Article 18 Budapest Convention on production orders with respect to subscriber information).

c Questions: Can current practices by US providers be generalised in a Protocol?

i. With regard to subscriber information?
ii. For disclosure of other data in emergency situations?

d Question: What rules/regulations or other factors prevent providers from voluntarily disclosing subscriber information to criminal justice authorities from other jurisdictions?

e Questions: Connecting factors: in what circumstances may service providers be subject to a domestic production order?

i. "Real and substantial connection" to a Party?
ii. Offering a service in the territory of a Party?
iii. Or otherwise "established" in the Party[4]?

f Questions regarding data protection and other safeguards for voluntary disclosure:

i. Which data protection and other safeguards apply:
   - Legal framework of country of service provider?
   - Legal framework of country of requesting criminal justice authority?
   - Legal framework of country where data is stored?
   - Legal framework of country of data subject? What if several countries are involved?

ii. On the part of the service provider as the data controller under European legal frameworks:
   - What conditions precisely have to be met to permit disclosure and which are the applicable provisions of the **GDPR** or Convention 108?

[3] See the report of the T-CY Cloud Evidence Group https://rm.coe.int/168064b77d
[4] See Court of Justice of the European Union, in particular cases regarding the "offering of a service" or the "directing of a service" towards an EU member State such as case C-131/12 (Google Spain), case C-230/14 (Weltimmo*), or* cases C-595/08 and C-144/09 (Pammer and Halpenof).
For a brief discussion of these cases see chapter 3.4 of T-CY(2016)5 https://rm.coe.int/16806a495e

- What would be considered a sufficient legal basis under the GDPR or Convention 108?
- What constitutes a "legitimate interest"[5] (Article 6.1.(f) GDPR) of a service provider in this context?
- What are requirements for disclosure/transfers of subscriber information to "third countries"?
- Would the derogations of Article 49 GDPR – such as Article 49.1 (f) – apply if data is required in a specific criminal investigation?
- What is the meaning of Article 48 GDPR?

iii. In the requesting country (that is, in the country of destination of data):
- What conditions precisely have to be met to permit transfer to this country and which are the applicable provisions of the **GDPR** or Convention 108?

iv. What data protection and other safeguards must be met for the voluntary disclosure of data in other jurisdictions?

▶ **Voluntary preservation of data by service providers**

– Brief review of current practices.[6]

g Question: Can current practices by US-providers be generalised in a Protocol?

▶ **Mandatory production orders**

– Brief overview of European Commission proposals for a European Production and Preservation Order[7] and how would this work within the European Union.

h Questions: Could such a mandatory regime be envisaged for non-EU countries?

i. For what type of data? Subscriber information only?
ii. What limitations and connecting factors?
iii. Role of competent authorities in requested country?
iv. Enforcement in case of non-compliance with order?
v. Safeguards and data protection requirements?

[5] See also WP 29: Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC http://www.dataprotection.ro/servlet/ViewDocument?id=1086
[6] See the report of the T-CY Cloud Evidence Group https://rm.coe.int/168064b77d
[7] Comprising proposals for a:
- Regulation on production orders https://ec.europa.eu/info/sites/info/files/placeholder.pdf
- Directive on legal representative https://ec.europa.eu/info/sites/info/files/placeholder_0.pdf

3.4 Lawful access to data in the cloud

– Brief discussion of the problem of loss of (knowledge of) location situations and the feasibility of mutual legal assistance.

▶ **Understanding jurisdiction: Connecting factors**

i Question: What may be relevant factors to determine jurisdiction to enforce (location of data or equipment in the territory of a State, and/or access by a person in the territory of a State who has "possession or control" of data)?

j Question: What is "transborder"?

▶ **Article 32 Budapest Convention**

– The limitations of Article 32 (see Guidance Note);

k Question: Is further clarification needed on the scope of Article 32?

▶ **Options**

The Guidance Note on Article 32 provides an example of "transborder" access:
"A suspected drug trafficker is lawfully arrested while his/her mailbox - possibly with evidence of a crime - is open on his/her tablet, smartphone or other device. If the suspect voluntarily consents that the police access the account and if the police are sure that the data of the mailbox is located in another Party, police may access the data under Article 32b."

l Question: What other scenarios could be envisaged?

- Scenarios?
- Risks?
- Conditions and safeguards?