www.coe.int/TCY

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, version 9 April 2013 T-CY (2013)13

Cybercrime Convention Committee (T-CY)

Invitation to a
Hearing of private sector and civil society stakeholders on transborder access to data

3 June 2013 (10h00 – 17h30)

Council of Europe

Room 9, Palais de l'Europe, Strasbourg, France

Note prepared by the T-CY Ad-hoc Subgroup on transborder access to data

Participation in the Hearing

The Hearing is open to representatives of

- civil society organisations,
- Internet Service Providers (including ISP associations),
- social media, cloud service providers,
- e-commerce platforms,
- online payment services
- members and observers in the Cybercrime Convention Committee (T-CY)
- and other interested stakeholders.

The Hearing will be held on

Monday, 3 June, from 10h00 to 17h30 in Room 9 of the Palais de l'Europe, Strasbourg, France (the main building of the Council of Europe)

Representatives of interested stakeholders are required to register beforehand in order to obtain badges for access to the building.

In order to facilitate and structure discussions, interested stakeholders are invited to submit written contributions addressing the issues listed in this note.

Stakeholders who are not able to participate in person are also invited to submit written contributions.

Deadline for **registration** and **written comments**: **15 May 2013**

For registration, written comments and further information please contact:

Marie Agha-Wevelsiep
Data Protection and Cybercrime Division
Council of Europe

Tel: +33-3-8841-2175
Mail: Marie.AGHA-WEVELSIEP@coe.int

1 Background

In November 2011, the Cybercrime Convention Committee (T-CY) decided to establish the "ad-hoc sub-group of the T-CY on jurisdiction and transborder access to data and data flows" (hereinafter, the "Transborder Group") with a view of developing an instrument "to further regulate the transborder access to data and data flows, as well as the use of transborder investigative measures on the Internet and related issues".

The Transborder Group was to examine in particular the use of Article 32b of the Convention, actual practices of transborder investigative measures and the challenges to transborder investigations under international law on jurisdiction and state sovereignty.

The report of the Transborder Group was adopted by the Cybercrime Convention Committee (T-CY) in December 2012.[1]

The report underlines that the increasing reliance of societies on ICT is accompanied by increasing offences against and by means of computer systems. Cybercrime violates the rights of individuals and, therefore, governments have the positive obligation to protect society against crime, among other things, through effective law enforcement.

The report notes that in order to meet this positive obligation, the need for transborder access – that is, for unilateral access by law enforcement authorities of one State to data stored on a computer system in a foreign State without the need for mutual legal assistance – has become more pressing for a variety of reasons, including the challenges related to cloud computing and thus of linking data (including electronic evidence – to a specific territory or jurisdiction.

The report also notes a number of concerns that would need to be addressed should possibilities for transborder access be enhanced. These range from legal and policy concerns to procedural safeguards protecting the rights of individuals, risks to the protection of personal data or implications for third parties.

The information provided in the report suggests that increasingly, law enforcement authorities access data stored on computers in other States in order to secure electronic evidence. Such practices may go beyond the limited possibilities foreseen in Article 32b (transborder access with consent) and the Budapest Convention in general.

The report as adopted by the T-CY proposes three solutions that should be pursued in parallel:

1. More effective use of the Budapest Convention in its current form, in particular with regard to its international cooperation provisions.
2. The preparation of a Guidance Note on Article 32 (transborder access to data) "to facilitate implementation of the Budapest Convention by the Parties, to correct misunderstandings regarding transborder access under this treaty, and to reassure third parties", in consultation with private sector entities.
3. The preparation of an Additional Protocol to the Budapest Convention on Cybercrime to allow for additional possibilities for transborder access to data.

[1] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/TCY_2012_3_transborder_rep_V31public_7Dec12.pdf

2 Objective

To seek the views of private sector entities and civil society

- on current practices and experiences regarding transborder access to data
- on a possible Additional Protocol to the Budapest Convention on Cybercrime.

The hearing is thus to inform the further work of the Cybercrime Convention Committee in this regard. The T-CY is seeking the views of non-governmental entities before work on a Protocol begins and will do so as it progresses.

3 Issues for discussion

Participants in the hearing are invited to address the following issues:

1. With regard to the current Article 32b of the Budapest Convention on transborder access, and as a private sector entity, what is your understanding and practical experience regarding:

    a. the notion of consent in this article
    b. the notion of a private entity being a person who lawfully can provide access or disclose data
    c. the type of data that can be disclosed by a private sector entity
    d. the conditions for disclosing data or providing access
    e. the notion of the person consenting to provide access or disclose data, especially in the situation where that person is somewhere else than in the territory of the requesting state.

2. With regard to the proposal to allow for enhanced possibilities for transborder access through an Additional Protocol to the Budapest Convention, what is your experience and what are your views on:

    a. the option of transborder access with consent but without the limitation to data stored "in another Party"
    b. the option of transborder access without consent but with lawfully obtained credentials
    c. the option of transborder access without consent in good faith or in exigent or other circumstances
    d. the option of extending a search from the original computer to connected systems without the limitation "in its territory" (Article 19.3 Budapest Convention)
    e. the power of disposal as connecting legal factor
    f. conditions and safeguards required
    g. other situations that should be covered by an Additional Protocol.

4 Appendix

4.1 Documentation

- Cybercrime Convention Committee (T-CY)/Ad-hoc Subgroup on Jurisdiction and Transborder Access to Data (2012): Transborder access and jurisdiction: What are the options? (T-CY(2012)3) http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/TCY2013/TCYreports/TCY_2012_3_transborder_rep_V31public_7Dec12.pdf

- Cybercrime Convention Committee (T-CY) (2013): (draft) T-CY Guidance Note #3 on Transborder Access to Data (article 32) (T-CY(2013)7) http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/TCY_2013_7E_GN3_transborder_V2public.pdf

- Cybercrime Convention Committee (T-CY) (2013): (draft) Note on Elements of an Additional Protocol on transborder access to data (T-CY(2013)14) http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY(2013)14transb_elements_protocol_V2.pdf

4.2 Article 32 Budapest Convention

Text of the provision:

> Article 32 – Trans-border access to stored computer data with consent or where publicly available
>
> A Party may, without the authorisation of another Party:
>
> a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
> b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Extract of the Explanatory Report:

> 293. The issue of when a Party is permitted to unilaterally access computer data stored in another Party without seeking mutual assistance was a question that the drafters of the Convention discussed at length. There was detailed consideration of instances in which it may be acceptable for States to act unilaterally and those in which it may not. The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules. Ultimately, the drafters decided to only set forth in Article 32 of the Convention situations in which all agreed that unilateral action is permissible. They agreed not to regulate other situations until such time as further experience has been gathered and further discussions may be held in light thereof. In this regard, Article 39, paragraph 3 provides that other situations are neither authorised, nor precluded.

294. Article 32 (Trans-border access to stored computer data with consent or where publicly available) addresses two situations: first, where the data being accessed is publicly available, and second, where the Party has accessed or received data located outside of its territory through a computer system in its territory, and it has obtained the lawful and voluntary consent of the person who has lawful authority to disclose the data to the Party through that system. Who is a person that is "lawfully authorised" to disclose data may vary depending on the circumstances, the nature of the person and the applicable law concerned. For example, a person's e-mail may be stored in another country by a service provider, or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data, as provided in the Article.