www.coe.int/TCY

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, version 5 November 2013 T-CY (2013)7 E

Cybercrime Convention Committee (T-CY)

T-CY Guidance Note # 3
Transborder access to data (Article 32)

Draft prepared by the Bureau for discussion by the T-CY

Comments on this draft Guidance Note should be sent to:

Alexander Seger		Tel	+33-3-9021-4506
Secretary Cybercrime Convention Committee		Fax	+33-3-9021-5650
Head of Data Protection and Cybercrime Division		Email	alexander.seger@coe.int
Directorate General of Human Rights and Rule of Law			
Council of Europe, Strasbourg, France			

1 Introduction

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[1]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The present Note addresses the question of transborder access to data under Article 32 Budapest Convention.[2]

Article 32b is an exception to the principle of territoriality and permits unilateral transborder access without the need for mutual assistance under limited circumstances. Parties are encouraged to make more effective use of all the international cooperation provisions of the Budapest Convention, including mutual assistance.

Overall, practices, procedures as well as conditions and safeguards vary considerably between different Parties. Concerns regarding procedural rights of suspects, privacy and the protection of personal data, the legal basis for access to data stored in foreign jurisdictions or "in the cloud" as well as national sovereignty persist and need to be addressed.

This Guidance Note is to facilitate implementation of the Budapest Convention by the Parties, to correct misunderstandings regarding transborder access under this treaty and to reassure third parties.

The Guidance Note will thus help Parties to take full advantage of the potential of the treaty with respect to transborder access to data.

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.

[1] See the mandate of the T-CY (Article 46 Budapest Convention).

[2] The preparation of this Guidance Note represents follow up to the findings of the report on "Transborder access and jurisdiction" (T-CY(2012)3) adopted by the T-CY Plenary in December 2012. http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/TCY2013/TCYreports/TCY_2012_3_transborder_rep_V31public_7Dec12.pdf

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.

3 T-CY interpretation of Article 32 Budapest Convention

With regard to Article 32a (transborder access to publicly available (open source) stored computer data) no specific issues have been raised and no further guidance by the T-CY is required at this point.

It is commonly understood that law enforcement officials may access any data that the public may access, and for this purpose subscribe to or register for services available to the public.[3]

If a portion of a public website, service or similar is closed to the public, then it is not considered publicly available in the meaning of Article 32a.

Regarding Article 32b, typical situations may include:

- 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.[4]

[3] Domestic law, however, may limit law enforcement access to or use of publicly available data.

[4] Paragraph 294 Explanatory Report.

- 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.

Other situations are neither authorised nor precluded.[5]

With regard to Article 32b (transborder access with consent) the T-CY shares the following common understanding:

3.1 General considerations and safeguards

Article 32b is a measure to be applied in specific criminal investigations and proceedings within the scope of Article 14.[6]

As pointed out above, it is presumed that the Parties to the Convention form a community of trust and that rule of law and human rights principles are respected in line with Article 15 Budapest Convention.[7]

---

[5] Paragraph 293 Explanatory Report. See also Article 39.3 Budapest Convention.

[6] Article 14 – Scope of procedural provisions
1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.
2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:
a the criminal offences established in accordance with Articles 2 through 11 of this Convention;
b other criminal offences committed by means of a computer system; and
c the collection of evidence in electronic form of a criminal offence.
3 a. Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.
b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:
i is being operated for the benefit of a closed group of users, and
ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

[7] Article 15 – Conditions and safeguards
1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

The rights of individuals and the interests of third parties are to be taken into account when applying the measure.

Therefore, a searching Party may consider notifying relevant authorities of the searched Party.

3.2 On the notion of "transborder" and "location"

Transborder access means to "unilaterally access computer data stored in another Party without seeking mutual assistance".[8]

The measure can be applied between the Parties.

Article 32b refers to "stored computer data located in another Party". This implies that Article 32b may be made use of if it is known where the data are located.

Article 32b would not cover situations where the data are not stored in another Party or where it is uncertain where the data are located. A party may not use article 32b to obtain disclosure of data that is stored domestically.

Article 32b "neither authorise[s], nor preclude[s]" other situations. Thus, in situations where it is unknown whether, or not certain that, data are stored in another Party, Parties may need to evaluate themselves the legitimacy of a search or other type of access in the light of domestic law, relevant international law principles or considerations of international relations.

3.3 On the notion of "access without the authorisation of another Party"

Article 32b does not require mutual assistance, and the Budapest Convention does not require a notification of the other Party. At the same time, the Budapest Convention does not exclude notification. Parties may notify the other Party if they deem it appropriate.

3.4 On the notion of "consent"

Article 32b stipulates that consent must be lawful and voluntary which means that the person providing access or agreeing to disclose data may not be forced or deceived.[9]

Subject to domestic legislation, a minor may not be able to give consent, or persons because of mental or other conditions may also not be able to consent.

---

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

[8] Paragraph 293 Explanatory Report to the Budapest Convention.

[9] In some countries, consenting to avoid or reduce criminal charges or a prison sentence also constitutes lawful and voluntary consent.

In most Parties, cooperation in a criminal investigation would require explicit consent. For example, general agreement by a person to terms and conditions of an online service used might not constitute explicit consent even if these terms and conditions indicate that data may be shared with criminal justice authorities in cases of abuse.

3.5 On the applicable law

In all cases, law enforcement authorities must apply the same legal standards under Article 32b as they would domestically. If access or disclosure would not be permitted domestically it would also not be permitted under Article 32b.

It is presumed that the Parties to the Convention form a community of trust and that rule of law and human rights principles are respected in line with Article 15 Budapest Convention.

3.6 On the person who can provide access or disclose data

As to "who" is the person who is "lawfully authorised" to disclose the data, this may vary depending on the circumstances, laws and regulations applicable.

For example, it may be a physical individual person, providing access to his email account or other data that he stored abroad.[10]

It may also be a legal person.

Service providers are highly unlikely to be able to consent validly and voluntarily to disclosure of their users' data under Article 32. Normally, service providers will only be holders of such data; they will not control or own the data, and they will, therefore, not be in a position validly to consent. Of course, law enforcement agencies may be able to procure data transnationally by other methods, such as mutual legal assistance or procedures for emergency situations.

3.7 Domestic lawful requests versus Article 32b

Article 32b is not relevant to domestic production orders or similar lawful requests internal to a Party.

3.8 On the location of the person consenting to provide access or disclose data

The standard hypothesis is that the person providing access is physically located in the territory of the requesting Party.

However, multiple situations are possible. It is conceivable that the physical or legal person is located in the territory of the requesting law enforcement authority when agreeing to disclose or actually providing access, or only when agreeing to disclose but not when providing access, or the person is located in the country where the data is stored when agreeing to disclose and/or providing access. The person may also be physically located in a third country when agreeing to cooperate or when actually providing access. If the person is a legal person (such as a private sector entity), this person may be represented in the territory of the requesting law enforcement authority, the territory hosting the data or even a third country at the same time.

[10] See the example given in Paragraph 294 Explanatory Report.

It should be taken into account that many Parties would object – and some even consider it a criminal offence – if a person who is physically in their territory is directly approached by foreign law enforcement authorities who seek his or her cooperation.

4 T-CY Statement

The T-CY agrees that the above represents the common understanding of the Parties as to the scope and elements of Article 32.