www.coe.int/TCY

Strasbourg, 3 December 2014
(Provisional)

T-CY (2014)16

Cybercrime Convention Committee (T-CY)

Transborder access to data and jurisdiction:

Options for further action by the T-CY

Report prepared by the

Ad-hoc Subgroup on Transborder Access and Jurisdiction

Adopted by the 12th Plenary of the T-CY (2-3 December 2014)

Contents

Contact

Alexander Seger
Executive Secretary of the Cybercrime Convention Committee (T-CY) Tel +33-3-9021-4506
Directorate General of Human Rights and Rule of Law Fax +33-3-9021-5650
Council of Europe, Strasbourg, France Email: alexander.seger@coe.int

1 Introduction

The present report has been prepared by the Transborder Group[1] of the Cybercrime Convention Committee (T-CY) in response to a decision taken by the 10th Plenary of the T-CY (2-3 December 2013).

The "Ad-hoc sub-group of the T-CY on jurisdiction and transborder access to data and data flows" (hereinafter, the "Transborder Group") was established by the Cybercrime Convention Committee (T-CY), at the 6th plenary session (23-24 November 2011).

The Transborder Group submitted a full report on "Transborder access to data and jurisdiction: what are the options?"[2] to the 8th T-CY Plenary which adopted the report on 6 December 2012.

That report underlined the need for transborder access, but also pointed at concerns and risks (legal and policy concerns, risks to procedural safeguards, implications for third parties, risks to the protection of personal data, risks to law enforcement operations) that would need to be addressed should powers for transborder access be enhanced, and lists a range of practices already applied, some of which are going beyond the limited possibilities foreseen in the Convention on Cybercrime.

The report proposed three solutions:

1. More effective use of the Budapest Convention, in particular its provisions on international cooperation;
2. A T-CY Guidance Note on Article 32;
3. An additional Protocol to the Convention on Cybercrime on access to electronic evidence.

The 8th Plenary extended the mandate of the Transborder Group to 31 December 2013. This led to:

- a public hearing in Strasbourg on 3 June 2013;
- a draft Guidance Note on Article 32;
- a decision by the 9th Plenary of the T-CY (June 2013) to commence work on a Protocol in 2014.

In December 2013, the Transborder Group submitted its report to the 10th Plenary of the T-CY and considered that:

- Further reflection and dialogue would be required with data protection authorities, civil society and private sector organisations in view of reconciling transborder access to data with safeguards and conditions to protect the rights of individuals and prevent misuse.
- While the Budapest Convention on Cybercrime is a criminal justice treaty covering specified criminal investigations within the scope of Article 14, the context of reports on mass surveillance by national security institutions could adversely affect the negotiation of a Protocol.

[1] "Ad-hoc sub-group on jurisdiction and transborder access to data and data flows"
[2] For the full report see:
http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/TCY_2012_3_transborder_rep_V31public_7Dec12.pdf

- The T-CY assessment of international cooperation provisions may lead to additional proposals to be reflected in a Protocol to the Budapest Convention.

The 10th Plenary of the T-CY followed this reasoning and decided:

> Agenda item 6: Transborder access to data
>
> To adopt the report presented by the Transborder Group for 2013[3]; and thus to request the Transborder Group:
> - to continue the dialogue with relevant stakeholders;
> - to take into account the results of the current round of T-CY assessments;
> - on this basis to submit a report with proposals to the 12th Plenary for consideration;
>
> pending consideration of this report to put on hold the decision taken at the 9th Plenary regarding the preparation of a Protocol to the Convention;

The present report summarises the results of the work undertaken by the Transborder Group[4] in 2014 and contains proposals for consideration by the 12th Plenary of the T-CY (December 2014).[5]

2 Activities in 2014

2.1 List of activities of the Transborder Group

The Transborder Group in 2014 carried out the following activities:

5-6 February 2014, Strasbourg	Meeting of the Transborder Group
28 May 2014, Strasbourg	Meeting with EU Data Protection Working 29, European Data Protection Supervisor and the Consultative Committee of Convention 108 (T-PD)
17 - 18 June 2014, Strasbourg	Briefing of the T-CY Plenary
19 - 20 June 2014, Strasbourg	Conference on data protection
24 September 2014, Brussels	Hearing at the Committee on Civil Liberties, Justice and Home Affairs of the EU Parliament (LIBE Committee)
8 - 9 October 2014, Strasbourg	Meeting of the Transborder Group

2.2 Meeting with representatives of data protection bodies

In December 2013, the T-CY received a letter from the EU Article 29 Working Party[6] on Data Protection with a series of comments arguing that the proposals discussed by the Transborder Group were not compatible with data protection regulations of the European Union.

[3] Document (T-CY(2013)30)
http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY(2013)30_Final_transb_rep_V5.pdf

[4] Members of the Transborder Group in 2014 included: Ioana Albani (Romania), Andrea Candrian (Switzerland), Markko Kunnapu (Estonia), Tsuyoshi Kitagawa (Japan), Erik Planken (Netherlands), Justin Millar (United Kingdom), Cristina Schulman (Romania), Betty Shave (USA), Branko Stamenkovic (Serbia) and Pedro Verdelho (Portugal).

[5] Note: The reports and its proposals were adopted by the 12th Plenary of the T-CY (2-3 December 2014).

[6] Article 29 Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p.31) sets up a Working Party on the Protection of Individuals with regard to the Processing of Personal Data. The "Article 29

The Transborder Group, therefore, on 28 May 2014 held a meeting with representatives of WP 29, the European Data Protection Supervisor and the Consultative Committee of Convention 108 (T-PD) to discuss the concerns expressed in the letter of WP 29 in detail.

Discussions confirmed the complexity of the question of transborder access to data and that the comments made by WP 29 in its letter may be valid for some but not for other scenarios.

Questions discussed included the following.

2.2.1 Criminal justice versus national security

The Parties to the Budapest Convention consider this a criminal law treaty that is to be used in specified criminal investigations and for specified data, and that it is not a treaty to be used for national security or mass surveillance purposes.

WP 29 questions this and points at the role of criminal justice authorities in national security measures and the sharing of data between criminal justice and national security authorities.

It should be clear that the Budapest Convention does not permit "blanket/mass transborder access, collection or transfer to/of data". Nevertheless, should the possibilities for transborder access for specified criminal investigations be enhanced, additional safeguards would need to be established.

2.2.2 The applicable data protection framework

WP 29 considers that Directive 95/46/EC[7] applies with regard to the transfer by private sector entities to law enforcement, while Framework Decision 2008/977/JHA[8] applies to international transfers of data between law enforcement authorities.

However, there is a range of open questions as to which data protection rules apply in a criminal law context.[9]

There are doubts as to why Directive 95/46/EC would be applicable if the question of transborder access were regulated in a criminal law treaty with its provisions transposed into domestic criminal law. The question was raised why this would not constitute a legitimate

---

Working Party" has advisory status and acts independently.
http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20131205_wp29_letter_to_cybercrime_committee.pdf

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[8] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:en:PDF

[9] Note Preamble of FD 2008/977/JHA:
"Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data does not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law, such as those provided for by Title VI of the Treaty on European Union, **nor, in any case, to processing operations concerning public security, defence, state security or the activities of the State in areas of criminal law.**"

derogation in line with Article 13 of Directive 95/46/EC or Article 9 of Data Protection Convention 108 of the Council of Europe.

Additional questions included whether it made a difference if data is transferred from private sector entities to law enforcement within EU member States, or from EU to non-EU States or from non-EU States to EU member States.

The discussion of this point remained inconclusive. Given the ongoing reform of the data protection framework within the European Union but also the Council of Europe[10], some of these questions may remain open for the time being.

2.2.3 Applicable law and safeguards

One of the most difficult points regarding transborder access to data seems to be the applicable law governing access.

WP 29 – in its letter of December 2013 – is of the opinion that the law of the searched State (State where data is accessed) applies:

- "The application of the requested Party's national law means that the requirements that need to be respected for national investigations will also need to be respected for cross-border investigations, and is therefore a guarantee for individuals' rights."
- "The EU data protection legislation ensures continuity of protection when EU data is transferred abroad. These safeguards for data processed in the EU cannot be circumvented by applying third countries' legislation to EU processed data."
- "An additional protocol to an international Convention that would appear to provide for access to data stored on computers abroad by applying the law (or the definitions of consent) of the searching party would be in violation of the EU data protection *acquis*."

Discussions:

- suggested that the approach that the law of the searched State applies may be valid with regard to some scenarios but may not necessarily ensure a higher level of protection of the rights of the individual in other situations;
- remained inconclusive as to the notion of "consent" which may be applied differently under data protection rules than in a criminal law context.

2.2.4 Ability of service providers to disclose data

WP 29 is of the opinion that a private sector entity functioning as data controller would not be able to disclose personal data voluntarily but only upon presentation of a judicial order.

The Transborder Group in principle agrees with this position. However, there may be situations where an Internet Service Provider or another data controller could disclose data (emergency situations, controller becomes aware of an offence, ISP is attacked, commercial rules, etc.). The statement that a data controller can "never" voluntarily disclose data would not be correct.

Section 3.6 of the draft Guidance Note (see appendix) reflects this understanding:

[10] http://www.coe.int/t/dghl/standardsetting/dataprotection/Cahdata_en.asp

> Service providers are 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.

2.2.5 Regulation or laissez-faire

It appears that an increasing number of countries – including within the EU – are adopting unilateral measures to obtain access to data stored in foreign or unknown locations for criminal justice purposes to protect individuals against crime, including offences against privacy (attacks against the confidentiality, integrity and availability of computers (articles 2 – 6 Budapest Convention) or offences such as cyberstalking or sextortion).

Discussions suggested a common understanding that relying on States to adopt their own, unilateral solutions carries the risk of a "jungle" situation while taking no action would lead to more crime and more violations of fundamental rights.

It would, therefore, be preferable to develop international solutions that allow for effective criminal justice measures with the necessary safeguards and conditions.

2.3 Conference on Article 15 safeguards and law enforcement access to data (19-20 June 2014)[11]

In December 2013, the T-CY decided to continue the dialogue with interested stakeholders. A Conference – organised under the project Cybercrime@Octopus – followed up on that decision and was organized in Strasbourg on June 19 and 20, 2014.

The conference discussed the following questions:

> Criminal justice authorities constantly and increasingly need electronic evidence from other countries for specific investigations. How should they obtain this evidence rapidly and consistent with rule of law and data protection requirements? How should they obtain such evidence in situations where mutual legal assistance procedures are not effective? More efficient international cooperation and adapting rules and procedures for securing volatile electronic evidence in an expedited manner are considered a matter of urgency.

In order to facilitate an exchange of views, the conference focused on:

- the distinction between specific investigations to secure data for specified criminal justice purposes versus surveillance and other activities of national security institutions;
- the challenge of law enforcement access to data in the light of technological developments and crime trends;
- data protection and other human rights and rule of law safeguards;
- possible solutions reconciling the obligation of governments to protect individuals and society against crime with safeguards.

[11] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/2014/3021_Art15Conf_Agenda_v8.pdf
http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/CyberCrime@Octopus/3021_art15Conf_Conclusions_v1e.pdf

The hearing showed the complexity of the matter with some participants rejecting any possibility for transborder access to data altogether, and with others underlining the need for common solutions taking account of technological changes, the evolution of cybercrime and of the need for clearer international rules to frame practices that are widespread already.

The hearing was to help identify solutions to transborder access to data while at the same time addressing concerns, such as the procedural rights of individuals and the protection of personal data. The hearing provided useful insights, for example, regarding limitations to voluntary consent by service providers to disclose data.

Importantly, the Transborder Group had prepared a range of case scenarios[12] in view of seeking guidance on applicable data protection rules in specific situations. These scenarios facilitated an open exchange of views, although the answers to the questions remained largely inconclusive.

The chair of the meeting summarised the conclusions of the conference as follows:

- The work of the T-CY on transborder access to data is part of a broad range of activities undertaken by the T-CY to support implementation of the Budapest Convention on Cybercrime to protect society and individuals against crime, to protect their rights and to promote the rule of law in cyberspace.
- It is understood that the Budapest Convention is a criminal law treaty that applies to specified criminal investigations and specified data.
- Access to electronic evidence in foreign jurisdictions is primarily governed by mutual legal assistance (MLA) arrangements. The current T-CY assessment of the functioning of the MLA provisions in view of enhancing their application is welcome.
- In the light of technological developments and the volatility of electronic evidence, MLA procedures are not always effective or useful. Data may be stored in unknown locations, be fragmented or moving between multiple locations or jurisdictions. This limits the ability of criminal justice authorities to protect society and individuals against crime.
- The Budapest Convention on Cybercrime – with Article 32 – allows for transborder access to data in limited situations.
- States increasingly develop unilateral solutions to access data in foreign or unknown jurisdictions beyond the provisions of the Budapest Convention. Common solutions are required to provide an international legal basis.
- Such solutions need to provide for safeguards, conditions and respect rule of law and human rights, including data protection, principles.
- Conditions include that powers to access data or permit transborder data flows are provided for by law, serve a legitimate aim and are necessary and proportionate in a democratic society. This will help avoid conflicts between data protection and criminal law.
- The principles and provisions of Data Protection Convention 108 and Recommendation R(87)15 may assist the T-CY in its further work. It was suggested that accession to Data Protection Convention 108 by Parties to the Budapest Convention would be welcome.
- Solutions are indeed required permitting criminal justice authorities to obtain electronic evidence in an effective manner and in compliance with data protection and rule of law

12 http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/CyberCrime@Octopus/cyber_COE_TB_Scenarios_june2014%20V5web.pdf

standards. The constructive dialogue to elaborate such solutions should therefore continue.

2.4 LIBE Committee hearing (24 September 2014)

On 12 February 2014, the Committee on Civil Liberties, Justice and Home Affairs of the EU Parliament had adopted a "report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs"[13] prepared by Rapporteur Claude Moraes.

While the report focuses on mass surveillance, it also includes strong criticism of the ongoing work of the T-CY on transborder access to data:

> *The European Parliament ….*
>
> 32. Stresses its serious concerns in relation to the work within the Council of Europe's Cybercrime Convention Committee on the interpretation of Article 32 of the Convention on Cybercrime of 23 November 2001 (Budapest Convention) on transborder access to stored computer data with consent or where publicly available, and opposes any conclusion of an additional protocol or guidance intended to broaden the scope of this provision beyond the current regime established by this Convention, which is already a major exception to the principle of territoriality because it could result in unfettered remote access by law enforcement authorities to servers and computers located in other jurisdictions without recourse to MLA agreements and other instruments of judicial cooperation put in place to guarantee the fundamental rights of the individual, including data protection and due process, and in particular Council of Europe Convention 108;

The report is based on extensive hearings and contributions by experts as reflected in Annex II of the report. However, the opinion of the T-CY had not been sought prior to the finalisation and adoption of the report.

In August 2014, the Secretariat of the LIBE Committee invited the T-CY Secretariat for a "mini-hearing" with LIBE in Brussels on 24 September 2014. The Chair of the T-CY, Erik Planken, and the Executive Secretary, Alexander Seger, addressed the LIBE Committee. Speakers also included Giovanni Buttarelli, Assistant European Data Protection Supervisor (EDPS), and Wojciech Wiewiórowski, Inspector General for Protection of Personal Data, Polish Data Protection Authority, Vice-Chair of the Article 29 Working Party. [14]

The hearing was rather controversial.

While the T-CY delegation underlined, among other things, that the Budapest Convention was a criminal justice treaty to be used in specific criminal investigations, that the purpose of a protocol would also be to prevent a "jungle" scenario and rogue assertions of jurisdiction by setting out a legitimate framework including safeguards and conditions, that the dialogue with data protection authorities and other stakeholders was sought to define such safeguards and conditions, that constructive solutions are needed to protect individuals against crime also in situations where mutual legal assistance was not applicable, and that there was no question of permitting "unfettered access" to data, members of the LIBE Committee maintained their position as already expressed in paragraph 32 of their report of February 2014.

[13] http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2014-0139&language=EN
[14] In October 2014, Mr. Buttarelli was appointed European Data Protection Supervisor ("EDPS"), and Mr. Wiewiórowski Assistant EDPS.

In conclusion it would seem that:

- the LIBE Committee used this opportunity to reassert its earlier position;
- the confusion between criminal justice and national security spheres prevails. General distrust in governments will make it difficult to negotiate new international agreements to address challenges that criminal justice authorities are faced with;
- the EU Parliament is unlikely to support negotiation of new agreements before the proposed data protection package is adopted. It would, therefore, be complicated for the EU Commission to obtain a negotiating mandate for a Protocol on transborder access to data.

2.5 T-CY assessment of international cooperation provisions

The Transborder Group – in its report of December 2012 – had stated that one solution would be a "more effective use of the Budapest Convention, in particular its provisions on international cooperation".

For this reason, the Transborder Group was tasked by the T-CY to take into account the results of the assessments of international cooperation provisions by the T-CY in 2013/2014.

The draft report on the T-CY assessment of Article 31 and related provisions contains a number of specific recommendations. Some are of a practical nature and could be implemented without delay, others require additional resources at domestic levels and others represent material for an additional Protocol to the Budapest Convention.

Some of the questions considered by the Transborder Group between 2012 and 2014 could be addressed in connection with follow up that is given to these recommendations.

2.6 Guidance Note on Article 32

The Transborder Group, in February 2013 prepared a draft Guidance Note for discussion in the public hearing and the 9th Plenary of the T-CY in June 2013.

Based on comments received in these meetings and further discussions within the Group, the Transborder Group prepared a new draft of the Guidance Note (version 9 October 2014).[15] This version:

- Underlines in Section 3.1 that Article 32b is a measure to be applied in specific criminal investigations and proceedings within the scope of Article 14 Budapest Convention.
- Notes in Section 3.6 that service providers would normally not be able to consent validly and voluntarily to the disclosure of users' data under Article 32b.
- States in Section 3.5 that LEA must not use Article 32b to take measures that would not be permitted under their domestic law.
- Notes in Section 3.7 that Article 32b is not relevant to domestic production orders.
- Suggests in Section 3.3 that Parties consider notifying relevant authorities of the searched Party. This is proposed as an additional safeguard to protect the rights of individuals and the interests of third parties.

[15] The draft Guidance Note is attached as an appendix and also available at: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/Guidance_Notes/T-CY%282013%297REV_GN3_transborder_V13.pdf

It is proposed that the T-CY Plenary consider this version of the draft Guidance Note in view of adoption.

3 Conclusions and options

3.1 Guidance Note on Article 32

It is proposed that the T-CY Plenary consider the draft Guidance Note in view of adoption.

3.2 Additional Protocol to the Convention on Cybercrime on transborder access to data

The Transborder Group considers that an additional Protocol on transborder access to data would be needed, but that such a Protocol is controversial in the current context.

The activities and analyses carried out by the Group suggest that a reasonable consensus to commence work on a Protocol is lacking.

On the one hand,

- criminal justice officials are extremely concerned and resentful about the difficulty of securing data for criminal justice purposes and of their limited ability to protect individuals and society against crime;

- as more people are online and as more activities take place online, more crime takes place online, more evidence is online and for many crimes evidence is only available online;

- electronic evidence is increasingly significant with regard to violent crime – including contract murder or rape arranged online, mass shootings, bombings, sextortion, stalking, or child abuse – that entails electronic evidence stored in foreign or unknown jurisdictions;

- the cost of such crime to human rights, including privacy, the impact of crime on victims and the positive obligation of governments to protect individuals against crime, including cybercrime, tends to be disregarded by many interlocutors. The lack of concern for the rights of victims has been a distressing revelation for the Transborder Group;

- technological developments, including cloud computing, use of multiple devices and platforms, or encryption, render the gathering of electronic evidence for criminal justice purposes highly complex;

- mutual legal assistance procedures are inefficient and are often not applicable;

- cooperation by providers is decreasing. There is a trend among providers not to cooperate with criminal justice officials even when permitted by law to do so, to notify accountholders of government inquiries, to understaff law enforcement compliance departments, and to delay complying with properly-issued court orders;

- an enormous percentage of leads and cases are abandoned because there is no realistic possibility of obtaining even basic data, such as who owns an IP address.

For these reasons, most officials responsible for criminal justice matters are in favour of expanding possibilities for transborder access to data for criminal justice purposes and with the necessary safeguards.

On the other hand,

- within many governments, some ministries may oppose transborder access to data if the data is located within their jurisdiction, while ignoring or tolerating that their own authorities access data in other jurisdictions;

- reports on mass surveillance and other activities of national security institutions have caused mistrust in governments and a confusion between the powers and activities of national security institutions with those of criminal justice authorities. Therefore, proposals to increase criminal justice powers will face public resistance. Many governments and parliaments will be reluctant to take this risk by negotiating a Protocol and transposing its provisions into domestic law;

- new data protection frameworks within the European and the Council of Europe are still in the making. The expectation that the EU would complete its work before mid-2014 did not materialise. Additional work on data protection regimes is underway, for example, between the EU and the USA ("Umbrella Agreement"[16]);

- in Europe, regulations on criminal justice access to data are unstable following the ruling of the European Court of Justice on the EU Data Retention Directive in April 2014;

- the question of transborder access to data is linked to the questions of jurisdiction. A number of recent developments suggest that this matter is fast evolving and may require further analysis.[17] T-CY 11 underlined "the importance of the question of jurisdiction, and thus to maintain Article 22 as a provision to be assessed in the following round of assessments".

For these reasons and within the current context, negotiation of a Protocol on transborder access to data would not be feasible.

At the same time, the problems listed above will not disappear but rather increase.

The Transborder Group believes that in the absence of an agreed upon international framework with safeguards, more and more countries will take unilateral action and extend law enforcement powers to remote transborder searches either formally or informally with unclear safeguards. Such unilateral or rogue assertions of jurisdiction will not be a satisfactory solution.

[16] http://ec.europa.eu/justice/data-protection/files/factsheets/umbrella_factsheet_en.pdf

[17] Examples:

- The ongoing YAHOO!/Belgium case.
- The "Marco Civil" adopted by the Brazilian Congress on 22 April 2014, puts Brazilian data under Brazilian jurisdiction regardless of where the data is stored. See Article 11 at http://www.internetjurisdiction.net/wp-content/uploads/2014/05/APPROVED-MARCO-CIVIL-MAY-2014-PROVIDED-BY-CGIbr.pdf
- US District Court ruling in April 2014 extending the reach of search warrant "to apply anywhere". http://www.theregister.co.uk/2014/04/28/us_judge_digital_search_warrants_apply_everywhere/ considering that inefficient MLA procedures to gain access to data on servers abroad would increase "the burden on the government [...] substantial, and law enforcement efforts would be seriously impeded".

Furthermore, as victimisation grows, the public will ask why governments are not able to obtain data in a reasonable and legitimate way when lives are in danger, and why justice frequently cannot be done.

The T-CY should, therefore, follow developments and reconsider the feasibility of a Protocol on the specific question of transborder access to data in the future.

3.3 Option for consideration by the T-CY

In the meantime the T-CY could pursue the following option:

As follow up to the work of the Transborder Group and the assessment of international cooperation provisions, the T-CY could consider setting up a working group on criminal justice access to evidence stored in the cloud, including through mutual legal assistance ("Cloud evidence group").

The main tasks of the group would be to explore solutions on criminal justice access to evidence stored on servers in the cloud and in foreign jurisdictions, including through mutual legal assistance.

The working group would prepare a report for consideration by the T-CY taking into account:

- the recommendations of the T-CY assessment report on the mutual legal assistance provisions of the Budapest Convention on Cybercrime (document T-CY(2013)17rev);
- the work of the Ad-hoc sub-group on transborder access to data and jurisdiction;
- a detailed description of the current situation and problems as well as emerging challenges regarding criminal justice access to data in the cloud and foreign jurisdiction.

The report should contain draft options and recommendations for further action by the T-CY.

The working group could be established for a period of two years (see appendix for the draft terms of reference).

4 Appendix

4.1 Draft Guidance Note on Article 32[18]

www.coe.int/TCY

Strasbourg, version 9 October 2014 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 Transborder Group for discussion by the T-CY

[18] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/Guidance_Notes/T-CY%282013%297REV_GN3_transborder_V13.pdf

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.[19]

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.[20]

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.

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

[20] 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.[21]

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.[22]

[21] Domestic law, however, may limit law enforcement access to or use of publicly available data.
[22] 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.[23]

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.[24]

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.[25]

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.

---

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

[24] 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.

[25] 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.
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.

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".[26]

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.[27]

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.

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.

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

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

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.[28]

It may also be a legal person.

Service providers are 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.

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.

---

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

4.2 Draft Terms of Reference of a "Cloud evidence group"

Name	Working group on criminal justice access to evidence stored in the cloud, including through mutual legal assistance ("Cloud evidence group")
Origin	T-CY Working Group under Article 1.1.j of the Rules of Procedure[29] established by decision of the T-CY [adopted at the 12th Plenary (2-3 December 2014)]
Duration	1 January 2015 – 31 December 2016
Main tasks	To explore solutions on criminal justice access to evidence stored on servers in the cloud and in foreign jurisdictions, including through mutual legal assistance. The Working Group shall prepare a report for consideration by the T-CY taking into account: • The recommendations of the T-CY assessment report on the mutual legal assistance provisions of the Budapest Convention on Cybercrime (document T-CY*2013)17rev). • The work of the Ad-hoc Sub-group on transborder access to data and jurisdiction. • A detailed description of the current situation and problems as well as emerging challenges regarding criminal justice access to data in the cloud and foreign jurisdiction. The report shall contain draft options and recommendations for further action by the T-CY.
Benchmarks and deliverables	• June 2015: Discussion paper with description of current and emerging challenges as basis for an exchange of views with service providers and other stakeholders at Octopus Conference 2015. • June 2015: Workshop at Octopus Conference. • December 2015: Interim report for consideration by the T-CY. • June 2016: Draft report for consideration by the T-CY. • December 2016: Final report for consideration by the T-CY.
Working methods	The Working Group shall hold its meetings back-to-back with meetings of the T-CY Bureau and in camera. The Working Group may hold public hearings, publish interim results and consult other stakeholders.
Composition	• Bureau members participate ex-officio with defrayal of cost[30] • Up to 5 additional members with defrayal of cost[31] • Additional T-CY members (State Parties) at their own cost.

[29] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY%282013%2925%20rules_v15.pdf
[30] Subject to the availability of funds.
[31] Subject to the availability of funds.