www.coe.int/TCY

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 1 March 2017 T-CY(2015)16

Cybercrime Convention Committee (T-CY)

T-CY Guidance Note #10

Production orders for subscriber information

(Article 18 Budapest Convention)

Adopted by the T-CY following the 16th Plenary by written procedure (28 February 2017)

Contact

Alexander Seger
Executive Secretary Cybercrime Convention Committee
Directorate General of Human Rights and Rule of Law
Council of Europe, Strasbourg, France

Tel +33-3-9021-4506
Fax +33-3-9021-5650
Email alexander.seger@coe.int

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]

While not binding, Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The present Note[2] addresses the question of production orders for subscriber information under Article 18, that is, situations in which:

- a person ordered to submit specified computer data is present in the territory of a Party (Article 18.1.a);[3]
- a service provider ordered to submit subscriber information is offering its services in the territory of the Party without necessarily being located in the territory (Article 18.1.b).

A Guidance Note on these aspects of Article 18 is relevant given that:

- subscriber information is the most often sought data in criminal investigations;
- Article 18 is a domestic power;
- the growth of cloud computing and remote data storage has raised a number of challenges for competent authorities seeking access to specified computer data – and, in particular, subscriber information – to further criminal investigations and prosecutions;
- currently, practices and procedures, as well as conditions and safeguards for access to subscriber information vary considerably among Parties to the Convention;
- concerns regarding privacy and the protection of personal data, the legal basis for jurisdiction pertaining to services offered in the territory of a Party without the service provider being established in that territory, as well as access to data stored in foreign jurisdictions or in unknown or multiple locations "within the cloud" need to be addressed.

The service and enforceability of domestic production orders against providers established outside the territory of a Party raises further issues which cannot be fully addressed in a Guidance Note. Some Parties may require that subscriber information be requested through mutual legal assistance.

Article 18 is a measure to be applied in specific criminal investigations and proceedings within the scope of Article 14 Budapest Convention. Orders are thus to be issued in specific cases with regard to specified subscribers.

[1] See the mandate of the T-CY (Article 46 Budapest Convention).
[2] This Guidance Note is based on the work of the T-CY Cloud Evidence Group.
[3] It is important to recall that Article 18.1.a of the Budapest Convention is not limited to subscriber information but concerns any type of specified computer data. This Guidance Note, however, addresses the production of subscriber information only.

2 Article 18 Budapest Convention[4]

2.1 Text of the provision

Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

Extract from the Explanatory Report:

173. Under paragraph 1(a), a Party shall ensure that its competent law enforcement authorities have the power to order a person in its territory to submit specified computer data stored in a computer system, or data storage medium that is in that person's possession or control. The term "possession or control" refers to physical possession of the data concerned in the ordering Party's territory, and situations in which the data to be produced is outside of the person's physical possession but the person can nonetheless freely control production of the data from within the ordering Party's territory (for example, subject to applicable privileges, a person who is served with a production order for information stored in his or her account by means of a remote online storage service, must produce such information). At the same time, a mere technical ability to access remotely stored data (e.g. the ability of a user to access through a network link remotely stored data not within his or her legitimate control) does not necessarily constitute "control" within the meaning of this provision. In some States, the concept denominated under law as "possession" covers physical and constructive possession with sufficient breadth to meet this "possession or control" requirement.

Under paragraph 1(b), a Party shall also provide for the power to order a service provider offering services in its territory to "submit subscriber information in the service provider's possession or control". As in paragraph 1(a), the term "possession or control" refers to subscriber information in the service provider's physical possession and to remotely stored subscriber information under the service provider's control (for example at a remote data storage facility provided by another company). The term "relating to such service" means that the power is to be available for the purpose of obtaining subscriber information relating to services offered in the ordering Party's territory.[5]

[4] See Appendix for Article 18 and extracts from the Explanatory Report in full.
[5] Paragraph 173 Explanatory Report.

2.2 What is "subscriber information?"

The term "subscriber information" is defined in Article 18.3 of the Budapest Convention:

> 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
>
> a the type of communication service used, the technical provisions taken thereto and the period of service;
>
> b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
>
> c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Paragraph 177 Explanatory Report furthermore notes:

> 177. "Subscriber information" is defined in paragraph 3. In principle, it refers to any information held by the administration of a service provider relating to a subscriber to its services. Subscriber information may be contained in the form of computer data or any other form, such as paper records. As subscriber information includes forms of data other than just computer data, a special provision has been included in the article to address this type of information. "Subscriber" is intended to include a broad range of service provider clients, from persons holding paid subscriptions, to those paying on a per-use basis, to those receiving free services. It also includes information concerning persons entitled to use the subscriber's account.

Obtaining subscriber information may represent a lesser interference with the rights of individuals than obtaining traffic data or content data.

2.3 What is a "service provider?"

The Budapest Convention on Cybercrime applies a broad concept of "service provider" which is defined in Article 1.c of the Budapest Convention.

For the purposes of this Convention:

> c "service provider" means:
>
> i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
>
> ii any other entity that processes or stores computer data on behalf of such communication service or users of such service.

Article 18.1.b is to be applied with respect to any service provider offering its services in the territory of the Party.[6]

[6] European Union instruments distinguish between providers of electronic communication services and of Internet society services. The concept of "service provider" of Article 1.c Budapest Convention encompasses both.

3 T-CY interpretation of Article 18 Budapest Convention with respect to subscriber information

3.1 The scope of Article 18.1.a

- The scope is broad: a "person" (which may include a "service provider") that is present in the Party's territory.
- With respect to computer data, the scope is broad but not indiscriminate: any "specified" computer data[2] (hence Article 18.1.a is not restricted to "subscriber information" and covers all types of computer data).
- The specified computer data is in that person's possession or, if the person has no physical possession, that person freely controls the computer data to be submitted under Article 18.1.a from within the Party's territory.
- The specified computer data is stored in a computer system or a computer-data storage medium.
- The production order is issued and enforceable by the competent authorities in the Party in which the order is sought and granted.

3.2 The scope of Article 18.1.b

The scope of Article 18.1.b is narrower than that of Article 18.1.a:

- Subsection b is restricted to a "service provider".[7]
- The service provider to which the order is issued is not necessarily present, but offers its services in the territory of the Party.
- It is restricted to "subscriber information."
- The subscriber information relates to such services and is in that service provider's possession or control.

In contrast to Article 18.1.a which is restricted in scope of application to "persons present in the territory of the Party", 18.1.b is silent on the issue of the location of the service provider. Parties could apply the provision in circumstances in which the service provider offering its services in the territory of the Party is neither legally nor physically present in the territory.

3.3 Jurisdiction

Article 18.1.b is restricted to circumstances in which the criminal justice authority issuing the production order has jurisdiction over the offence.

This may include situations in which the subscriber is or was resident or present in that territory when the crime was committed.

The present interpretation of Article 18 is without prejudice to broader or additional powers under the domestic law of Parties.

Agreement to this Guidance Note does not entail consent to the extraterritorial service or enforcement of a domestic production order issued by another State nor creates new obligations or relationships between the Parties.

[7] The "person" is a broader concept than "a service provider", although a "service provider" can be "a person".

3.4 What are the characteristics of a "production order?"

A "production order" under Article 18 is a domestic measure and is to be provided for under domestic criminal law. A "production order" is constrained by the adjudicative and enforcement jurisdiction of the Party in which the order is granted.

Production orders under Article 18 refer:

> to computer data or subscriber information that are in the possession or control of a person or a service provider. The measure is applicable only to the extent that the person or service provider maintains such data or information. Some service providers, for example, do not keep records regarding the subscribers to their services.[8]

The Explanatory Report[9] to the Budapest Convention refers to production orders as a flexible measure which is less intrusive than search or seizure or other coercive powers and further states that:

> the implementation of such a procedural mechanism will also be beneficial to third party custodians of data, such as ISPs, who are often prepared to assist law enforcement authorities on a voluntary basis by providing data under their control, but who prefer an appropriate legal basis for such assistance, relieving them of any contractual or non-contractual liability.

3.5 What effect does the location of the data have?

The storage of subscriber information in another jurisdiction does not prevent the application of Article 18 Budapest Convention as long as such data is in the possession or control of the service provider. The Explanatory Report states with respect to:

- Article 18.1.a that "the term 'possession or control' refers to physical possession of the data concerned in the ordering Party's territory, and situations in which the data to be produced is outside of the person's physical possession but the person can nonetheless freely control production of the data from within the ordering Party's territory."[10]

- Article 18.1.b that "the term 'possession or control' refers to subscriber information in the service provider's physical possession and to remotely stored subscriber information under the service provider's control (for example at a remote data storage facility provided by another company)."[11]

Regarding Article 18.1.b, a situation may include a service provider that has its headquarters in one jurisdiction, but stores the data in another jurisdiction. Data may also be mirrored in several jurisdictions or move between jurisdictions according to service provider discretion and without the knowledge or control of the subscriber. Legal regimes increasingly recognise that, both in the criminal justice sphere and in the privacy and data protection sphere, the location of the data is not the determining factor for establishing jurisdiction.

[8] Paragraph 172 Explanatory Report.
[9] Paragraph 171 Explanatory Report.
[10] Paragraph 173 Explanatory Report. A "person" in Article 18.1.a Budapest Convention may be a physical or legal person, including a service provider.
[11] Paragraph 173 Explanatory Report.

3.6 What is "offering its services in the territory of a Party?"

The growth of cloud computing has raised questions as to when a service provider is considered to be offering its services in the territory of the Party and thus may be issued a domestic production order for subscriber information. This has led to a range of interpretations across multiple jurisdictions by courts in both civil and criminal cases.

With regard to Article 18.1.b, Parties could consider that a service provider is "offering its services in the territory of the Party", when:

- the service provider enables persons in the territory of the Party to subscribe to its services[12] (and does not, for example, block access to such services);

and

- the service provider has established a real and substantial connection to a Party. Relevant factors include the extent to which a service provider orients its activities toward such subscribers (for example, by providing local advertising or advertising in the language of the territory of the Party), makes use of the subscriber information (or associated traffic data) in the course of its activities, interacts with subscribers in the Party, and may otherwise be considered established in the territory of a Party.

The sole fact that a service provider makes use of a domain name or electronic mail address connected to a specific country does not create a presumption that its place of business is located in that country. Therefore, the requirement that the subscriber information to be produced is relating to services of a provider offered in the territory of the Party may be considered to be met even if those services are provided via a country code top-level domain name referring to another jurisdiction.

3.7 General considerations and safeguards

The Parties to the Convention are expected to form a community of trust that respects Article 15 Budapest Convention.

> 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 against 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.

[12] Note Paragraph 183 Explanatory Report: "The reference to a "service agreement or arrangement" should be interpreted in a broad sense and includes any kind of relationship on the basis of which a client uses the provider's services."

3.8 Applying Article 18 with respect to subscriber information

The production of subscriber information under Article 18 Budapest Convention could, therefore, be ordered if the following criteria are met in a specific criminal investigation and with regard to specified subscribers:

<table>
<tr><td colspan="3">IF
The criminal justice authority has jurisdiction over the offence;</td></tr>
<tr><td colspan="3">AND IF
the service provider is in possession or control of the subscriber information;</td></tr>
<tr><td colspan="3">AND IF</td></tr>
<tr><td>Article 18.1.a
The person (service provider) is in the territory of the Party.</td><td>OR</td><td>Article 18.1.b
A Party considers that a service provider is “offering its services in the territory of the Party” when, for example:

– the service provider enables persons in the territory of the Party to subscribe to its services (and does not, for example, block access to such services);
and
– the service provider has established a real and substantial connection to a Party. Relevant factors include the extent to which a service provider orients its activities toward such subscribers (for example, by providing local advertising or advertising in the language of the territory of the Party), makes use of the subscriber information (or associated traffic data) in the course of its activities, interacts with subscribers in the Party, and may otherwise be considered established in the territory of a Party.</td></tr>
<tr><td colspan="3">AND IF</td></tr>
<tr><td></td><td></td><td>– the subscriber information to be submitted is relating to services of a provider offered in the territory of the Party.</td></tr>
</table>

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 18 Budapest Convention with respect to the production of subscriber information.

5 Appendix: Extracts of the Budapest Convention

Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;

b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Explanatory Report

Production order (Article 18)

170. Paragraph 1 of this article calls for Parties to enable their competent authorities to compel a person in its territory to provide specified stored computer data, or a service provider offering its services in the territory of the Party to submit subscriber information. The data in question are stored or existing data, and do not include data that has not yet come into existence such as traffic data or content data related to future communications. Instead of requiring States to apply systematically coercive measures in relation to third parties, such as search and seizure of data, it is essential that States have within their domestic law alternative investigative powers that provide a less intrusive means of obtaining information relevant to criminal investigations.

171. A "production order" provides a flexible measure which law enforcement can apply in many cases, especially instead of measures that are more intrusive or more onerous. The implementation of such a procedural mechanism will also be beneficial to third party custodians of data, such as ISPs, who are often prepared to assist law enforcement authorities on a voluntary basis by providing data under their control, but who prefer an appropriate legal basis for such assistance, relieving them of any contractual or non-contractual liability.

172. The production order refers to computer data or subscriber information that are in the possession or control of a person or a service provider. The measure is applicable only to the extent that the person or

service provider maintains such data or information. Some service providers, for example, do not keep records regarding the subscribers to their services.

173. Under paragraph 1(a), a Party shall ensure that its competent law enforcement authorities have the power to order a person in its territory to submit specified computer data stored in a computer system, or data storage medium that is in that person's possession or control. The term "possession or control" refers to physical possession of the data concerned in the ordering Party's territory, and situations in which the data to be produced is outside of the person's physical possession but the person can nonetheless freely control production of the data from within the ordering Party's territory (for example, subject to applicable privileges, a person who is served with a production order for information stored in his or her account by means of a remote online storage service, must produce such information). At the same time, a mere technical ability to access remotely stored data (e.g. the ability of a user to access through a network link remotely stored data not within his or her legitimate control) does not necessarily constitute "control" within the meaning of this provision. In some States, the concept denominated under law as "possession" covers physical and constructive possession with sufficient breadth to meet this "possession or control" requirement.

Under paragraph 1(b), a Party shall also provide for the power to order a service provider offering services in its territory to "submit subscriber information in the service provider's possession or control". As in paragraph 1(a), the term "possession or control" refers to subscriber information in the service provider's physical possession and to remotely stored subscriber information under the service provider's control (for example at a remote data storage facility provided by another company). The term "relating to such service" means that the power is to be available for the purpose of obtaining subscriber information relating to services offered in the ordering Party's territory.

174. The conditions and safeguards referred to in paragraph 2 of the article, depending on the domestic law of each Party, may exclude privileged data or information. A Party may wish to prescribe different terms, different competent authorities and different safeguards concerning the submission of particular types of computer data or subscriber information held by particular categories of persons or service providers. For example, with respect to some types of data, such as publicly available subscriber information, a Party might permit law enforcement agents to issue such an order where in other situations a court order could be required. On the other hand, in some situations a Party might require, or be mandated by human rights safeguards to require that a production order be issued only by judicial authorities in order to be able to obtain certain types of data. Parties may wish to limit the disclosure of this data for law enforcement purposes to situations where a production order to disclose such information has been issued by judicial authorities. The proportionality principle also provides some flexibility in relation to the application of the measure, for instance in many States in order to exclude its application in minor cases.

175. A further consideration for Parties is the possible inclusion of measures concerning confidentiality. The provision does not contain a specific reference to confidentiality, in order to maintain the parallel with the non-electronic world where confidentiality is not imposed in general regarding production orders. However, in the electronic, particularly on-line, world a production order can sometimes be employed as a preliminary measure in the investigation, preceding further measures such as search and seizure or real-time interception of other data. Confidentiality could be essential for the success of the investigation.

176. With respect to the modalities of production, Parties could establish obligations that the specified computer data or subscriber information must be produced in the manner specified in the order. This could include reference to a time period within which disclosure must be made, or to form, such as that the data or information be provided in "plain text", on-line or on a paper print-out or on a diskette.

177. "Subscriber information" is defined in paragraph 3. In principle, it refers to any information held by the administration of a service provider relating to a subscriber to its services. Subscriber information may be contained in the form of computer data or any other form, such as paper records. As subscriber information includes forms of data other than just computer data, a special provision has been included in the article to

address this type of information. "Subscriber" is intended to include a broad range of service provider clients, from persons holding paid subscriptions, to those paying on a per-use basis, to those receiving free services. It also includes information concerning persons entitled to use the subscriber's account.

178. In the course of a criminal investigation, subscriber information may be needed primarily in two specific situations. First, subscriber information is needed to identify which services and related technical measures have been used or are being used by a subscriber, such as the type of telephone service used (e.g., mobile), type of other associated services used (e.g., call forwarding, voice-mail, etc.), telephone number or other technical address (e.g., e-mail address). Second, when a technical address is known, subscriber information is needed in order to assist in establishing the identity of the person concerned. Other subscriber information, such as commercial information about billing and payment records of the subscriber may also be relevant to criminal investigations, especially where the crime under investigation involves computer fraud or other economic crimes.

179. Therefore, subscriber information includes various types of information about the use of a service and the user of that service. With respect to the use of the service, the term means any information, other than traffic or content data, by which can be established the type of communication service used, the technical provisions related thereto, and the period of time during which the person subscribed to the service. The term 'technical provisions' includes all measures taken to enable a subscriber to enjoy the communication service offered. Such provisions include the reservation of a technical number or address (telephone number, web site address or domain name, e-mail address, etc.), as well as the provision and registration of communication equipment used by the subscriber, such as telephone devices, call centers or LANs (local area networks).

180. Subscriber information is not limited to information directly related to the use of the communication service. It also means any information, other than traffic data or content data, by which can be established the user's identity, postal or geographic address, telephone and other access number, and billing and payment information, which is available on the basis of the service agreement or arrangement between the subscriber and the service provider. It also means any other information, other than traffic data or content data, concerning the site or location where the communication equipment is installed, which is available on the basis of the service agreement or arrangement. This latter information may only be relevant in practical terms where the equipment is not portable, but knowledge as to the portability or purported location of the equipment (on the basis of the information provided according to the service agreement or arrangement) can be instrumental to an investigation.

181. However, this article should not be understood as to impose an obligation on service providers to keep records of their subscribers, nor would it require service providers to ensure the correctness of such information. Thus, a service provider is not obliged to register identity information of users of so-called prepaid cards for mobile telephone services. Nor is it obliged to verify the identity of the subscribers or to resist the use of pseudonyms by users of its services.

182. As the powers and procedures in this Section are for the purpose of specific criminal investigations or proceedings (Article 14), production orders are to be used in individual cases concerning, usually, particular subscribers. For example, on the basis of the provision of a particular name mentioned in the production order, a particular associated telephone number or e-mail address may be requested. On the basis of a particular telephone number or e-mail address, the name and address of the subscriber concerned may be ordered. The provision does not authorise Parties to issue a legal order to disclose indiscriminate amounts of the service provider's subscriber information about groups of subscribers e.g. for the purpose of data-mining.

183. The reference to a "service agreement or arrangement" should be interpreted in a broad sense and includes any kind of relationship on the basis of which a client uses the provider's services. _____