COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

16 September 2016
Strasbourg, France

T-CY (2016)5
Provisional

Cybercrime Convention Committee (T-CY)

Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY

Final report of the T-CY Cloud Evidence Group

www.coe.int/cybercrime

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

Contents

1 Background and purpose of this report

1 The Cybercrime Convention Committee (T-CY), at its 12th plenary (2-3 December 2014), established a working group to explore solutions for access to evidence in the cloud for criminal justice purposes, including through mutual legal assistance ("Cloud Evidence Group").[1]

2 This decision was motivated by the recognition that in the light of the proliferation of cybercrime and other offences involving electronic evidence, and in the context of technological change and uncertainty regarding jurisdiction, additional solutions are required to permit criminal justice authorities to obtain specified electronic evidence in specific criminal investigations.

3 The Cloud Evidence Group was tasked to submit a report to the T-CY with options and recommendations for further action by the end of 2016. It was to base its work on:

- 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).[2]
- The work of the Ad-hoc Sub-group on transborder access to data and jurisdiction.[3]
- 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.

4 Solutions should remain within the scope of Article 14 Budapest Convention[4], that is, cover specified data within specific criminal investigations. They will not pertain to bulk interception of data or other measures for national security purposes.

5 Given the interest of the European Union in this topic, the Cloud Evidence Group sought close coordination with EU institutions, including in particular the Netherlands Presidency of the EU in the first half of 2016.[5]

6 The present report represents the final report of the Cloud Evidence Group for submission to the T-CY. It summarises the challenges, issues and solutions identified by the Cloud Evidence Group and comprises a set of recommendations for consideration by the T-CY.

---

[1] Document T-CY(2014)16: Transborder Access to data and jurisdiction: Options for further action by the T-CY (report of the Transborder Group adopted by the 12th Plenary of the T-CY, December 2014).
[2] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c
[3] http://www.coe.int/en/web/cybercrime/tb
[4] 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.
…..
[5] In June 2016, the Justice and Home Affairs Council of the European Union adopted a set of measures to improve criminal justice in cyberspace. These measures were inspired by the work and preliminary results of the T-CY Cloud Evidence Group.
http://www.consilium.europa.eu/en/press/press-releases/2016/06/09-criminal-activities-cyberspace/
See also references to the need for efficient access to electronic evidence in
http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf
http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf

Activities of the Cloud Evidence Group

Strasbourg, 3-4 February 2015	Meeting of the Cloud Evidence Group
Klingenthal, 6-7 May 2015	Meeting of the Cloud Evidence Group and finalization of the discussion on Challenges
Strasbourg, 15-16 June 2015	T-CY Plenary: presentation of the discussion paper on "Challenges"
Strasbourg, 17-19 June 2015	Octopus Conference: Workshop on cloud evidence
The Hague, 28-30 September 2015	Meeting of the Cloud Evidence Group at EUROPOL with representatives of EU COM/DG Home, Working Party 29, EUROJUST, EUROPOL and European Court of Justice
Strasbourg, 30 November 2015	Hearing of service providers
Strasbourg, 1-2 December 2015	T-CY Plenary: Update on the work of the Cloud Evidence Group
Freiburg, 7-9 February 2016	Meeting of the Cloud Evidence Group at the Max-Planck Institute
Amsterdam, 7-8 March 2016	Participation by some members of the CEG and the T-CY Secretariat in the Amsterdam Conference on jurisdiction in cyberspace with presentation of "issues and options"
Brussels, 24-25 April 2016	Meeting of the Cloud Evidence Group and exchange of views with service providers and representatives of the European Commission
Strasbourg, 3 May 2016	Finalisation of a Background Paper on "Cooperation with foreign service providers"
Strasbourg, 23 May 2016	Exchange of views with data protection organisations
Strasbourg, 24-25 May 2016	T-CY Plenary: Presentation of draft options and recommendations
Strasbourg, 12-14 September 2016	Meeting of the Cloud Evidence Group and informal meeting with members of the European Union Parliament
Strasbourg, 14-15 November 2016	T-CY Plenary: Submission of final draft report for consideration by the T-CY
Strasbourg, 16-18 November 2016	Presentation of findings at Octopus Conference

Documents prepared by the Cloud Evidence Group

T-CY(2015)10 26 May 2015	Criminal justice access to data in the cloud: challenges[6]
T-CY(2015)21 18 February 2016	Application of Article 18.1.b Budapest Convention on "production order": Compilation of replies to the questionnaire[7]
T-CY(2016)7 17 February 2016	Criminal justice access to electronic evidence in the cloud – Informal summary of issues and options under consideration by the Cloud Evidence Group[8]
T-CY(2016)2 3 May 2016	Criminal justice access to data in the cloud: Cooperation with "foreign" service providers[9]
T-CY(2015)16 4 May 2016	Draft Guidance Note on Production Orders[10]
T-CY(2016)13 4 May 2016	Emergency requests for immediate disclosure of data: compilation of replies to the questionnaire.[11]

[6] http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b59
[7] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805a0873
[8] http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805a53c8
[9] http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064b77d
[10] http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064b77c
[11] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680651a6f

2 Challenges

7 In May 2015, the Cloud Evidence Group released a discussion paper on "Criminal justice access to data in the cloud: challenges"[12] in order to facilitate deliberations within the T-CY, the Octopus Conference 2015[13] and other fora and to seek the cooperation of industry and other stakeholders in identifying solutions.

8 Subsequent reflections, cases and reports confirm that analysis of challenges which is summarised here.

2.1 Scale and quantity of cybercrime, devices, users and victims

9 The current scale, scope and challenges related to cybercrime and electronic evidence (that is, evidence in the form of data generated by or stored on a computer system) are such that cybercrime has become a serious threat to the fundamental rights of individuals, to the rule of law in cyberspace and to the functioning of democratic societies. Cybercrime affects the right to private life and the protection of personal data, it endangers the property of citizens and industry, it represents attacks against dignity and integrity of individuals and in particular children, it involves attacks against media, civil society organisations and individuals and thus against the freedom of expression, it means attacks against governments, parliaments and other democratic institutions as well as public infrastructure and thus attacks against democracy, it represents attacks against democratic stability in that information and communication technologies are misused for xenophobic and racist purposes and contribute to radicalisation and terrorism, and it threatens international peace and stability in that military conflicts and political disagreements are often accompanied by cyberattacks.

10 Cybercrime is not a peripheral matter but a primary concern to governments, societies and individuals given the dependency on ICT and the trillions of security incidents on networks each year and millions of attacks against computers and data per day.

11 Beyond cybercrime per se, evidence in relation to any crime now often stored in electronic form on computer systems and often in foreign, unknown, multiple or shifting jurisdictions. Most international requests for data are thus related to fraud and financial crime followed by violent and serious crime ranging from murder, assault, smuggling of persons, trafficking in human beings, sextortion and other sexual crimes, drug trafficking, money laundering, terrorism and the financing of terrorism, extortion and, in particular, child pornography and other forms of sexual exploitation and abuse of children.

12 Predictions are that cybercrime as well as other crime involving electronic evidence will increase significantly with every month.

2.2 Ensuring the rule of law in cyberspace

13 Cybercrime, the number of devices, services and users (including of mobile devices and services) and with these the number of victims have reached proportions so that only a minuscule share of cybercrime or other offences involving electronic evidence will ever be recorded and investigated. The vast majority of victims of cybercrime cannot expect that justice will be served. This threatens the rule of law and the ability of governments to meet their obligations to protect society against crime and to protect the rights of victims.[14]

[12] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b59
[13] http://www.coe.int/en/web/cybercrime/octopus2015
[14] On the obligation of Governments to protect individuals against crime, including through criminal law, see European Court of Human Rights in K.U. v. Finland https://www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/K.U.%20v.%20FINLAND%20en.pdf

14 Because, as just noted, physical-world crime increasingly entails electronic evidence, the rule of law is threatened not only in cyberspace but in the physical world. Ultimately, this decreasing ability to investigate, and to defend public safety and human rights, will mean, on the one hand, vigilantism or victims without justice and, on the other, criminals gathering money and power and corrupting democratic government.

15 A major reason for this risk to the rule of law is the complexity of securing data as evidence in criminal proceedings:

- Technical challenges in this respect are, among other things, related to Virtual Private Networks, anonymizers (such as TOR), encryption, voice-over-Internet-protocol or Carrier-grade Network Addressing Translators (CGN) during the transition from Internet Protocol Version 4 to IPv6. These issues are not within the scope of the work of the Cloud Evidence Group.

- Legal and jurisdictional challenges are in particular related to cloud computing.

2.3 Cloud computing, territoriality and jurisdiction[15]

16 "Cloud computing" means that data is less held on a specific device or in closed networks but is distributed over different services, providers, locations and often jurisdictions. Issues include:

- Independence of location is a key characteristic of cloud computing. Therefore:

  - It is often not obvious for criminal justice authorities in which jurisdiction the data is stored and/or which legal regime applies to data. A service provider may have its headquarters in one jurisdiction and apply the legal regime of a second jurisdiction while the data is stored in a third jurisdiction. Data may be mirrored or backed up in several, or move between jurisdictions. If the location of data determines the jurisdiction, it is conceivable that a cloud service provider systematically moves data to prevent criminal justice access. Or, the provider may not easily know the location of the data.
  - Even if theoretically data may always have a location also when stored on cloud servers, it is far from clear which rules apply for lawful access by criminal justice authorities. It may be argued that the location of the headquarters of the service provider, or of its subsidiary, or the location of the data and server, or the law of the State where the suspect has subscribed to a service, or the location or citizenship of the suspect may determine jurisdiction.
  - It is often not clear whether a cloud provider is the "controller" or the "processor" of the data of a user and thus which rules apply.
  - Additional jurisdictional issues arise, for example, when the data owner is unknown or when the data is stored via transnational co-hosting solutions.

- A service provider may be under different layers of jurisdictions for various legal aspects related to its service at the same time. For example:

  - For data protection purposes, within EU member States, jurisdiction seems to be decided by the location of the data controller (even if the processing takes place outside the European Union) or by the location of processing of the data of data subjects in the EU (even if the controller or processor is not established in the EU) if the processing is related to the offering of goods or services to such data subjects in the EU.[16]

[15] For a more detailed and annotated version of this section see the "Challenges" report of May 2015 at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b59

  - For tax purposes, jurisdiction seems not decided by the location of the international HQ, servers or data controllers, but on several other criteria, such as the location of the subsidiary doing business.
  - With regard to consumer protection, the location of the consumer seems preferable.
  - For intellectual property rights in civil cases the location of the business seems to determine jurisdiction, while for intellectual property in criminal law the location of the perpetrator may be decisive.
  - In anti-trust cases, EU competition authorities are recommended to extend searches from a computer of a company or its subsidiary within the EU to computers in foreign jurisdictions in order to collect evidence.
  - Service providers may set up complex business arrangements through which a third party may become the trustee of their data so as to insulate themselves from legal process.
  - Or service providers may organise themselves so that they appear to have no headquarters or physical presence and thereby evade any jurisdiction.

- The sharing and pooling of resources is a key characteristic of cloud computing. Cloud services may entail a combination of service models (Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), and Cloud Infrastructure as a Service (IaaS)). In such cases, it is often unclear which service provider is in possession or control of which type of data (subscriber information, traffic data, content data) so as to be served a production order.

- Cloud service providers may take the position that governments must serve lawful orders not on them but on the owners of the data. This often means that law enforcement must attempt to serve a series of companies or litigate whether a company actually has control of the data, all while trying to keep the target – which may be the company in control of the data – from destroying the data when it learns of the investigation.

- It is often unclear whether data is stored or in transit and thus whether production orders, search and seizure orders, interception or real-time collection orders are to be served.

- It is not always clear whether different types of cloud services are considered and regulated as “electronic communication services” or “information society services”. This has implications on the type of and conditions for procedural law powers that can be applied.

- Regarding interceptions (obtaining content under Articles 21 and 34 Budapest Convention) specific problems arise. For example:

  - A court order served to a service provider domestically to intercept an electronic communication between two suspects on its territory and/or its nationals, is often not executable in real time because the server where the interception is to take place is located in a foreign jurisdiction or the communication is routed via a foreign jurisdiction. The foreign authorities are unlikely to respond to an MLA request in real time, given the duration of procedures and the requirements for interception in that country, unless emergency procedures are in place. In the case of the USA, US authorities cannot obtain content in real-time for foreign authorities.

[16] See Article 3 of the General Data Protection Regulation (GDPR) and Article 4 of current Directive 95/46/EC.

- A court order may be served for the interception of a communication of a national suspect. However, the suspect moves to another country or moves between different countries. It may be unclear whether the interception is legally possible when the suspect is in roaming.

- The non-localised nature of cloud computing causes problems for live forensics (online forensics) and searches because of the architecture of the cloud (multi tenancy, distribution and segregation of data) as well as legal challenges related to the integrity and validity of the data collection, evidence control, ownership of the data or jurisdiction.

2.4 Mutual legal assistance

17 Mutual legal assistance remains the principal means to obtain evidence from foreign jurisdictions for use in criminal proceedings. In December 2014, the Cybercrime Convention Committee (T-CY) completed an assessment of the functioning of mutual legal assistance provisions.[17] It concluded, among other things, that:

> The mutual legal assistance (MLA) process is considered inefficient in general, and with respect to obtaining electronic evidence in particular. Response times to requests of six to 24 months appear to be the norm. Many requests and thus investigations are abandoned. This adversely affects the positive obligation of governments to protect society and individuals against cybercrime and other crime involving electronic evidence.

18 The Committee adopted a set of recommendations to make the process more efficient. These recommendations should be implemented.

19 At the same time, MLA is not always a realistic solution to access evidence in the cloud context, or it may per se be unavailable, for the reasons indicated above.

2.5 Questions raised

20 The "challenges" paper in the end raised a number of questions relating to jurisdiction and mutual legal assistance:

- Which government would be the addressee of a lawful request for data by a country attacked in a cloud context where the territorial origin of a cyber-offence is not clear, the controller of data is hidden behind layers of service providers, or data is moving, fragmented or mirrored in multiple jurisdictions?

- What governs jurisdiction to enforce for criminal justice purposes: Location of data? Nationality of owner of data? Location of owner of data? Nationality of data owner? Location of data controller? Headquarters of a cloud service provider? Subsidiary of a cloud service provider? Territory where a cloud provider is offering its services? Laws of the territory where the data owner has subscribed to a service? Territory of the criminal justice authority? Degree to which the provider is active in the territory?

- What does "offering its services in a territory" mean (see Article 18.1.b Budapest Convention)[18]?

[17] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf

[18] 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,

- If a domestic court order authorizes the interception of a communication between two nationals or persons on its territory, why would MLA be required even if technically the provider would carry out the interception on a server in a foreign country? To what extent would the sovereignty of that foreign country be affected? To what extent would the rights of the defendants not be protected? Similarly for production orders regarding content data?

- Is it realistic that the number of MLA requests sent, received and processed can be increased by a factor of hundred or thousand or ten thousand? Are governments able to dramatically increase the resources available for the efficient processing of mutual legal assistance requests not only at the level of competent central authorities but also at the level of local courts, prosecution and police offices where MLA requests are prepared and executed?

- What would be a reasonable timeframe to obtain data from a foreign authority? Could this be defined in a binding agreement?

- Is it conceivable to develop a light regime for subscriber information, e.g. expedited disclosure?

- What additional international legally binding solutions could be considered to allow for efficient criminal justice access to specified data in foreign or unknown jurisdictions within the framework of specific criminal investigations?[19]

21 The specific issues identified and the options proposed in response by the Cloud Evidence Group would provide answers to some of these questions.

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.

[19] See, for example, Recommendations 19 to 24 on page 127 of http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf

3 Specific issues to be addressed

22 The T-CY Cloud Evidence Group considers that the following specific issues need to be addressed.

3.1 Mutual legal assistance

23 Where electronic evidence is stored in foreign jurisdictions, mutual legal assistance in criminal matters is the primary means to obtain evidence. In 2013 and 2014, the T-CY carried out a detailed assessment of the mutual legal assistance provisions of the Budapest Convention. In December 2014, the Committee adopted a report with a set of recommendations to improve the efficiency of mutual legal assistance.[20] The CEG is of the opinion that this assessment and its recommendations remain valid.

24 The report concludes that overall, [21]

> expeditious mutual legal assistance (MLA) is one of the most important conditions for effective measures against cybercrime and other offences involving electronic evidence given the transnational and volatile nature of electronic evidence. In practice, however, current mutual legal assistance procedures are considered too complex, lengthy and resource intensive, and thus too inefficient.
>
> ...
>
> Response times to requests of six to 24 months appear to be the norm. Many requests and thus investigations are abandoned. This adversely affects the positive obligation of governments to protect society and individuals against cybercrime and other crime involving electronic evidence.
>
> ...
>
> And yet, Parties appear not to make full use of the opportunities offered by the Budapest Convention on Cybercrime and other agreements for the purposes of effective mutual legal assistance related to cybercrime and electronic evidence.

25 It furthermore concludes that not all types of data are needed with the same frequency or urgency:

> In terms of the type of data requested, subscriber information has been singled out as the most often sought information. The large amount of requests for such information puts a heavy burden on authorities responsible for processing and executing MLA requests and slows down – and often prevents – criminal investigations. This suggests that solutions to the challenge of subscriber information would render MLA more efficient.

26 In December 2014, the T-CY thus adopted a set of recommendations to make the MLA process regarding cybercrime and electronic evidence more efficient through more effective use of existing provisions of the Budapest Convention on Cybercrime and other agreements but also by proposing additional solutions. [22]

[20] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c
[21] See page 122 of the report at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c
[22] See page 125 to 127 of the report at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c

27 For example,

- Parties should fully implement the preservation powers of the Budapest Convention (Recommendation 1), monitor the effectiveness of the MLA process (Rec 2), allocate more and better trained staff and more resources for MLA (Rec 3 and 4), strengthen the role and capacities of 24/7 points of contact (Rec 5), establish procedures for emergency situations (Rec 8) and so on.

- The Council of Europe, through capacity building projects should develop online tools and standardized multi-language templates for Article 31-requests for stored data (Rec 17 and 18).

- Parties should consider – possibly through a Protocol to the Budapest Convention – allowing for the expedited disclosure of subscriber information (Rec 19), the possibility of international production orders (Rec 20), direct cooperation between judicial authorities (Rec 21), addressing the practice of directly obtaining information from foreign service providers (Rec 22), joint investigations and/or joint investigative teams between Parties (Rec 23), allowing for requests to be sent in English language (Rec 24).

28 The T-CY has begun to review follow-up given to Recommendations 1 to 18.[23] Recommendations 19 to 24 and Recommendation 8 on emergency situations[24] will be discussed below among the options that could be pursued.

3.2 Differentiating between types of data sought

29 For the purposes of criminal investigations, three types of data may be needed:

- "Subscriber information"[25], that is, information to identify the user of a specific Internet Protocol (IP) address or, vice versa, the IP addresses used by a specific person. Subscriber information also comprises data from registrars on registrants of domains.

- "Traffic data"[26], that is, log files that record activities of the operating system of a computer system or of other software or of communications between computers, especially source and destination of messages.

- "Content data" such as emails, images, movies, music, documents or other files.[27] A distinction should be made between "stored" content, that is, data already available on a computer system and "future" content that is not yet available and will have to be obtained in real time.

---

[23] See T-CY 15 in May 2016 http://www.coe.int/en/web/cybercrime/t-cy-plenaries

[24] http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680651a6f

[25] The term "subscriber information" is defined in Article 18.3 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,[25] 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."

[26] as defined in Article 1.d Budapest Convention:
"d 'traffic data' means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service;"

[27] According to paragraph 209 of the Explanatory Report of the Budapest Convention:
"'Content data' is not defined in the Convention but refers to the communication content of the communication; i.e., the meaning or purport of the communication, or the message or information being conveyed by the communication (other than traffic data)."

30 Subscriber information is the most often sought information in domestic and international criminal investigations relating to cybercrime and electronic evidence as underlined by Parties in the T-CY assessment report of 2014. Without this information, it is often impossible to proceed with an investigation. It is therefore crucial to address the issue of obtaining subscriber information.

31 Subscriber information generally is evaluated as being less privacy sensitive than traffic data and content data. As a consequence most criminal law systems establish strict safeguards regarding law enforcement access to content and in particular the interception of communications.

32 Traffic data as well is considered sensitive as underlined, for example, by the European Court of Justice in connection with the issue of data retention.[28]

33 Subscriber information is normally held by private sector service providers and is typically obtained by law enforcement through production orders.[29] The procedural power of a production orders represent a lesser interference with the rights of individuals and the interests of third parties than the powers of search and seizure of computer systems or the interception of communications.

34 In the light of this and given that the Budapest Convention makes a distinction between subscriber information, traffic data and content data, the CEG is of the opinion that establishing a separate regime for access to subscriber information will highly contribute to making the MLA process regarding cybercrime and electronic evidence more efficient. Article 18 Budapest Convention already provides for a legal basis.

> 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.

35 However, several issues would need to be addressed in this context:

- Rules on obtaining subscriber information differ between Parties to the Budapest Convention. The T-CY reviewed procedures for obtaining subscriber information in 2014[30] and concluded that while most of the Parties that participated in the exercise made a distinction in their definition or concepts between "subscriber information" and "traffic data":
  - "In most of the responding Parties, the conditions for obtaining subscriber information appear to be the same or similar to those for obtaining traffic data,

[28] http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf
"The Court observes first of all that the data to be retained make it possible, in particular, (1) to know the identity of the person with whom a subscriber or registered user has communicated and by what means, (2) to identify the time of the communication as well as the place from which that communication took place and (3) to know the frequency of the communications of the subscriber or registered user with certain persons during a given period. Those data, taken as a whole, may provide very precise information on the private lives of the persons whose data are retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, activities carried out, social relationships and the social environments frequented.
The Court takes the view that, by requiring the retention of those data and by allowing the competent national authorities to access those data, the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data."
[29] See Article 18 Budapest Convention.
[30] http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7ad1

in particular if subscriber information is related to a dynamic IP address.[31] In more than half of these Parties, obtaining subscriber information requires judicial authorisation, and in others a prosecutor or an authorised senior law enforcement officer can order the production of subscriber information.

- In other Parties, the requirements for obtaining subscriber information are lower than those for traffic data, and the production of subscriber information can be ordered by the police or a prosecutor."

- This diversity of approaches adversely affects domestic investigations and international cooperation. The report, adopted by the T-CY in December 2014, therefore, recommended that the T-CY "facilitate greater harmonisation between the Parties on the conditions, rules and procedures for obtaining subscriber information"; and "encourage Parties to take account of the observations of this report when reforming their domestic regulations."

36 The CEG furthermore highlights that the Justice and Home Affairs Council of the European Union, in its "Council conclusions on improving criminal justice in cyberspace" adopted on 9 June 2016[32], states that:

> "enhancing cooperation with service providers or any other comparable solution that allows for quick disclosure of data should be considered; less rigorous legal process could be envisaged for obtaining specific categories of data, in particular subscriber data …"

37 This conclusion implies a distinction between different types of data in domestic laws and in corresponding rules regarding access to or disclosure of different types of data, including of subscriber information as opposed to traffic data.

38 As the Internet has no borders as such, subscriber information needed in an investigation may be held by a service provider "offering its services in the territory" of a Party although the provider may actually be located and the information sought may be stored on servers in other jurisdictions.[33] The CEG is of the opinion that a logical interpretation of Article 18.1.b Budapest Convention offers a solution. The competent authorities of a Party should be able to request subscriber information from a service provider offering a service in its territory irrespective of where the information is stored and where the provider is located. This important implication will be discussed further below as a separate point.

---

[31] A reason as to why some Parties treat access to subscriber information (in particular for dynamic IP addresses) and traffic data in the same way seems to be that in some European instruments traffic data and subscriber information are lumped together. See for example the categories of data to be retained under Article 5 of the former EU Data Retention Directive 2006/24/EC (http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32006L0024&from=EN). The Directive was declared invalid by the European Court of Justice in 2014.
The E-Privacy Directive of 2002 defined "Traffic data" defined as:
"Article 2 (b) "traffic data" means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;" . That Directive does not offer a separate definition of "subscriber information" which seems to be partially subsumed under "traffic data" (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML The Directive was amended in 2009. The revised consolidated version is here: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:PDF)

[32] http://www.consilium.europa.eu/en/press/press-releases/2016/06/09-criminal-activities-cyberspace/

[33] For example, Google has also several data centres in Europe (http://www.google.com/about/datacenters/inside/locations/index.html), Microsoft has "more than 100 data centers" including in Amsterdam and Dublin http://download.microsoft.com/download/8/2/9/8297F7C7-AE81-4E99-B1DB-D65A01F7A8EF/Microsoft_Cloud_Infrastructure_Datacenter_and_Network_Fact_Sheet.pdf, and Facebook also has a datacentre in Sweden https://www.facebook.com/LuleaDataCenter

3.3 "Loss of location"

39 Mutual legal assistance presupposes that the location of the data sought is known and that it is thus feasible and known to which State and to which competent authority to address an MLA request.

40 Under the conditions of cloud computing this is often not the case as indicated in the section on "cloud computing, territoriality and jurisdiction" above:

- It is often not obvious for criminal justice authorities in which jurisdiction the data is stored and/or which legal regime applies to data. A service provider may have its headquarters in one jurisdiction and apply the legal regime of a second jurisdiction while the data is stored in a third jurisdiction. Data may be mirrored in several or move between jurisdictions. If the location of data determines the jurisdiction, it is conceivable that a cloud service provider systematically moves data to prevent criminal justice access.

- Even if theoretically data may always have a location also when stored on cloud servers, it is far from clear which rules apply for lawful access by criminal justice authorities. It may be argued that the location of the headquarters of the service provider, or of its subsidiary, or the location of the data and server, or the law of the State where the suspect has subscribed to a service, or the location or citizenship of the suspect may determine jurisdiction.

41 Thus, for example,

- even if a server farm were located in the territory of a State, the authorities of that State would not have sufficient indications that the specific data sought are on those servers to obtain a search warrant. Even if they had a search warrant, they might not be able to access the data because of encryption, and the encryption keys might be held by a legal or natural person in another jurisdiction;

- when the origin of an attack is concealed and unknown to criminal justice, trace-back techniques may risk leading investigators to routers and servers in unknown jurisdictions;

- in situations where a computer on a crime scene or of a person being investigated is "live" (that is operating and active), criminal justice authorities could technically access data (including those stored on cloud servers) without knowledge of the jurisdiction in which the server is located and the data is stored.

42 Law enforcement powers are normally determined by the principle of territoriality. Under this principle, no State may enforce its jurisdiction in the territory of another sovereign State.[34] Criminal justice access to data on servers or computer systems in general located in other jurisdictions without the involvement of the authorities of those jurisdictions raises concerns.

43 At the same time, in "loss of (knowledge of) location" situations, the principle of territoriality is difficult to apply, in particular if it is to be based on the location of the data sought.

[34] Cf. Case of the S.S. "Lotus" (France v. Turkey), PCIJ Series A, No. 10
See also page 10 of one of the report of the T-CY Transborder Group at
http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8

44 Article 32b of the Budapest Convention on Cybercrime offers a solution only for very limited situations as described in the Guidance Note adopted by the T-CY in December 2014.[35] The Guidance Note mentions two example for illustration:

- 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.

- 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.

45 As noted by the T-CY previously, given these limitations and in the absence of a clear, efficient and feasible international legal framework, governments increasingly pursue unilateral solutions in practice. It seems to be widespread practice that law enforcement in a specific criminal investigation access data not only on the device of the suspect but also on connected devices such as email or other cloud service accounts if the device is open or the access credentials have been obtained lawfully even if they know that they are connecting to a different, known country.

46 In order to reduce risks to State-to-State relations and defend the rights of individuals, including their safety, a common international solution is required to provide a framework for lawful transborder access to data. Such a framework may focus less on the location of the data but on the location of the person in possession or control of the data.

47 The location of the victim at the time of the crime in the territory of a Party may also support a claim for jurisdiction and if needed (unilateral) transborder access to data, within agreed upon limitations.

48 For example, if a physical or legal person under investigation is present in the territory and thus within the jurisdiction of a criminal justice authority, the authority would be able to lawfully access or order the production of data in possession or control of that person also transborder.

49 In this connection, the CEG looked into the long-arm doctrine of EU anti-trust law (Cases *ICI* 48/69; *Woodpulp* 89/85) and noted that the European Commission recommends that competition authorities within the European Union obtain access to servers anywhere in the world to gather evidence in anti-trust proceedings:[36]

> 5. Practice shows that undertakings may store, access or otherwise use business related information on external servers or other storage media such as so-called cloud services (networked online storage where data is stored on multiple virtual servers) which are located outside the territory of the competent national competition authority or outside the European Union. To have effective powers to gather digital evidence, it is important that the Authorities can in the exercise of their inspection powers gather digital information which is accessible to the undertaking or person whose premises are being inspected irrespective of where it is stored, including on servers or other storage media located outside the territory of the respective national competition authority or outside the European Union.
> ...

[35] http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726a
[36] European Competition Network "Recommendation on the power to collect digital evidence, including by forensic means" http://ec.europa.eu/competition/ecn/ecn_recommendation_09122013_digital_evidence_en.pdf

It is recommended that:

1. All Authorities should have effective and efficient powers to gather digital evidence, including evidence obtained forensically, through inspections of business and/or nonbusiness premises, requests for information and other investigative tools. To that end, the Authorities should have the power to gather all information in digital form related to the business(es) under investigation, irrespective of the medium on which it is stored and the technological evolution of the storage media. The Authorities should also have powers to gather digital information by taking digital copies, including forensic images, of the data held and/or through the seizure of storage media.

2. The power to gather digital evidence, including evidence obtained forensically, as set out in Recommendation 1, should include the right to access information which is accessible to the undertaking or person whose premises are being inspected and which is related to the business(es) under investigation.

50 A framework on transborder access will need to define conditions and safeguards for such access to data in order to protect the rights of individuals and prevent prejudice to the powers or rights of other governments or their subjects (as understood under the concept of “comity”).

51 Solutions to address “loss of location” situations are also under discussion within the European Union. The Justice and Home Affairs Council of the EU, in its “Council conclusions on improving criminal justice in cyberspace” adopted on 9 June 2016[37], states that:

> Rules on enforcement jurisdiction should be reviewed
> … in situations where existing frameworks are not sufficient, e.g. situations where a number of information systems are used simultaneously in multiple jurisdictions to commit one single crime, situations where relevant e-evidence moves between jurisdictions in short fractions of time, or where sophisticated methods are used to conceal the location of e-evidence or the criminal activity, leading to "loss of location".[38]

3.4 A service provider in the territory or offering a service in the territory of a State

52 As indicated above, a major challenge of cloud computing is that data is not stable but often distributed over and moving between different services, providers, locations and jurisdictions, while law enforcement powers are usually defined territorially.

53 A criminal justice authority can thus either establish jurisdiction to enforce by focusing on the location of the computer system or storage device (this is covered by the search and seizure provisions of Article 19 Budapest Convention) or of the natural or legal person (including service providers) in possession or control of the data sought.[39] The latter is covered by Article 18 on production orders:

[37] http://www.consilium.europa.eu/en/press/press-releases/2016/06/09-criminal-activities-cyberspace/
[38] The European Commission has since launched a survey among EU Member States https://ec.europa.eu/eusurvey/runner/eevidence
[39] Given the volatility of data location, there seems to be a tendency to determine jurisdiction less on the basis of the location of data or computer systems but on the basis of the location of the person in possession or control. For example, European Union Directive 2016/1148 on the security of network and information systems (“NIS Directive”) of 6 July 2016 provides for jurisdiction as follows:

“Article 18 Jurisdiction and territoriality
1. For the purposes of this Directive, a digital service provider shall be deemed to be under the jurisdiction of the Member State in which it has its main establishment. A digital service provider shall be deemed to have its main establishment in a Member State when it has its head office in that Member State.
2. A digital service provider that is not established in the Union, but offers services referred to in Annex III

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.

54 The Budapest Convention uses a broad concept of "service provider".[40] According to Article 1c:

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.

within the Union, shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. The digital service provider shall be deemed to be under the jurisdiction of the Member State where the representative is established.
3. The designation of a representative by the digital service provider shall be without prejudice to legal actions which could be initiated against the digital service provider itself."

Recital 64 reads:
"(64) Jurisdiction in respect of digital service providers should be attributed to the Member State in which the digital service provider concerned has its main establishment in the Union, which in principle corresponds to the place where the provider has its head office in the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect. This criterion should not depend on whether the network and information systems are physically located in a given place; the presence and use of such systems do not, in themselves, constitute such main establishment and are therefore not criteria for determining the main establishment."
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

[40] Unlike current EU instruments which differentiate between Electronic Communication Service Providers and Information Society Service Providers. Within the context of a reform of the E-Privacy Directive, this distinction is in question. https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-commission-launches-public-consultation-kick-start-review

55 Article 18 Budapest Convention offers an important tool to address some of the problems of cloud computing. While under Article 18.1.a any natural or legal person in the territory of a Party could be ordered by the competent authorities of that Party to produce any type of data, Article 18.1.b is limited to service providers "offering a service in the territory of the Party" which are to produce subscriber information only.

56 The Explanatory Report (paragraph 173) to the Budapest Convention indicates that the actual location of the data is not relevant:

> 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.

57 The Explanatory Report (paragraph 171) furthermore indicates that the production order of Article 18 would also be useful for service providers which are prepared to cooperate voluntarily with law enforcement authorities:

> 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.

58 With regard to Article 18.1.b and the production of subscriber information by a service provider offering a service in the territory of a Party, the Cloud Evidence Group discussed the case law of the Court of Justice of the European Union, in particular cases regarding the "offering of a service" or the "directing of a service" towards an EU member State such as case C-131/12 (Google Spain), case C-230/14 (Weltimmo)[41], *or* cases C-595/08 and C-144/09 (Pammer and Halpenof).

59 In the data protection case Google Spain versus Costeja, the Court of Justice of the European Union discussed the question of the territorial application of EU Directive 95/46 and stated that:

> "Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State."[42]

[41] Judgment rendered on 1 October 2015
http://curia.europa.eu/juris/document/document.jsf?text=&docid=168944&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=222584
Hungarian language Web-based platform
–Consumers post their ads for real properties located in Hungary
–Servers located in Germany
–Platformed owned by Slovak entity, with no activity in Slovakia, no presence in Hungary except bank account, PO Box and a representative involved in the settlement of disputes
Issue: Is Weltimmo subject to Hungarian law?

[42] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN

60 In the civil law cases Pammer and Halpenof, the Court of Justice of the European Union determined "whether a trader whose activity is presented on its website or on that of an intermediary can be considered to be 'directing' its activity to the Member State of the consumer's domicile, within the meaning of Article 15(1)(c) of Regulation No 44/2001", and stated that:

> … it should be ascertained whether, before the conclusion of any contract with the consumer, it is apparent from those websites and the trader's overall activity that the trader was envisaging doing business with consumers domiciled in one or more Member States, including the Member State of that consumer's domicile, in the sense that it was minded to conclude a contract with them.
>
> The following matters, the list of which is not exhaustive, are capable of constituting evidence from which it may be concluded that the trader's activity is directed to the Member State of the consumer's domicile, namely the international nature of the activity, mention of itineraries from other Member States for going to the place where the trader is established, use of a language or a currency other than the language or currency generally used in the Member State in which the trader is established with the possibility of making and confirming the reservation in that other language, mention of telephone numbers with an international code, outlay of expenditure on an internet referencing service in order to facilitate access to the trader's site or that of its intermediary by consumers domiciled in other Member States, use of a top-level domain name other than that of the Member State in which the trader is established, and mention of an international clientele composed of customers domiciled in various Member States. It is for the national courts to ascertain whether such evidence exists.
>
> On the other hand, the mere accessibility of the trader's or the intermediary's website in the Member State in which the consumer is domiciled is insufficient. The same is true of mention of an email address and of other contact details, or of use of a language or a currency which are the language and/or currency generally used in the Member State in which the trader is established. [43]

61 In the data protection case Weltimmo (C-230/14)[44] the Court of Justice of the European Union underlined that the concept of "establishment" or "to be established" is to be defined in a flexible manner:

> 28 With regard, in the first place, to the concept of 'establishment', it should be noted that recital 19 in the preamble to Directive 95/46 states that establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements and that the legal form of such an establishment, whether simply a branch or a subsidiary with a legal personality, is not the determining factor (judgment in Google Spain and Google, C-131/12, EU:C:2014:317, paragraph 48). Moreover, that recital states that, when a single controller is established on the territory of several Member States, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities.
>
> 29 As the Advocate General observed, in essence, in points 28 and 32 to 34 of his Opinion, this results in a flexible definition of the concept of 'establishment', which departs from a formalistic approach whereby undertakings are established solely in the place where they are registered. Accordingly, in order to establish whether a company, the data controller, has an establishment, within the meaning of Directive 95/46, in a Member State other than the Member State or third country where it is registered, both the degree of stability of the arrangements and the effective exercise of activities in that other Member State must be interpreted in the light of the specific nature of the economic activities and the provision of

[43] Judgment rendered on 7 December 2010. http://curia.europa.eu/juris/liste.jsf?language=en&num=C-585/08

[44] http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=lst&docid=168944&occ=first&dir=&cid=21880

> services concerned. This is particularly true for undertakings offering services exclusively over the Internet.
> 30 In that regard, it must, in particular, be held, in the light of the objective pursued by that directive, consisting in ensuring effective and complete protection of the right to privacy and in avoiding any circumvention of national rules, that the presence of only one representative can, in some circumstances, suffice to constitute a stable arrangement if that representative acts with a sufficient degree of stability through the presence of the necessary equipment for provision of the specific services concerned in the Member State in question.
> 31 In addition, in order to attain that objective, it should be considered that the concept of 'establishment', within the meaning of Directive 95/46, extends to any real and effective activity — even a minimal one — exercised through stable arrangements.

62 The CEG noted with interest legal provisions in the Philippines which define "doing business" in Section 1 of RA 5455[45] as follows:

> … the phrase doing business shall include soliciting orders, purchases, service contracts, opening offices, whether called liaison offices or branches; appointing representatives or distributors who are domiciled in the Philippines or who in any calendar year stay in the Philippines for a period or periods totalling one hundred eighty days or more; participating in the management, supervision or control of any domestic business firm, entity or corporation in the Philippines; and any other act or acts that imply a continuity of commercial dealings or arrangements, and contemplate to that extent the performance of acts or works, or the exercise of some of the functions normally incident to, and in progressive prosecution of, commercial gain or of the purpose and object of the business organization.

63 An example studied by the Cloud Evidence Group was the case of Belgium versus Yahoo! on which the Supreme Court of Belgium took a final decision on 1 December 2015.[46] The decision is summarized here:

> On 1 December 2015, the Belgian Supreme Court issued a final decision that Yahoo! Inc. registered in California, USA, is obliged to produce subscriber information and is thus subject to the coercive measure of Article 46bis of the Belgian Rules of Criminal Procedure.
>
> Yahoo! Inc. had appealed against an earlier decision of the Court of Appeals of Antwerp of 20 November 2013, among other reasons that under international customary law a State has no extraterritorial jurisdiction to enforce.
>
> The Belgian Supreme Court ruled that:
>
> - Article 46bis §2 of the Belgian Rules of Criminal Procedure was indeed a coercive measure. Refusal to cooperate is punishable with a fine.
> - In general, a State can enforce coercive measures only on its own territory and would otherwise violate the sovereignty of a another State
> - "A State imposes a measure of coercion on its own territory as far as there is, between that measure and that territory, a sufficient territorial link."
> - Article 46bis §2 of the Belgian Rules of Criminal Procedure "only intends to enforce upon operators and suppliers active in Belgium a measure with a view to obtain mere identification data on the occasion of a crime or offence, the investigation of which falls within the competency of the Belgian prosecution authorities. This measure does not require a presence abroad of the Belgian

[45] Entitled *An Act To Require That The Making Of Investments And The Doing of Business Within The Philippines By Foreigners Or Business Organizations Owned In Whole Or In Part By Foreigners Should Contribute To The Sound And Balanced Development Of The National Economy On A Self-Sustaining Basis, And For Other Purpose.* Approved on 30 September 1968.
[46] http://jure.juridat.just.fgov.be/pdfapp/download_blob?idpdf=N-20151201-1

> Police or Magistrates, nor of agents acting on their behalf. This measure neither requires any material action or act abroad. The measure therefore has a restricted scope and bearing, the execution of which does not require any intervention outside of Belgian territory".
> - Yahoo! Inc., "as a supplier of a free webmail service, is present on Belgian territory and voluntarily subjects himself to Belgian law as he actively participates in Belgian economic life, by specifically using the domain name 'www.yahoo.be', the use of the local language, showing publicity based on the location of the users of his services and his reachability in Belgium for these users by installing a complaint box and FAQ desk."
> - "The Public Prosecutor does not require anything in the United States from an American subject, but requires something in Belgium from an American subject offering services on Belgian territory".
> - There was, therefore, no exercise of extraterritorial jurisdiction.

64 This ruling thus makes the case that an order for the production of subscriber information to a provider offering and thus being "present" in the territory of a Party is a domestic order (as is Article 18.1.b) and not a matter of international cooperation or exercise of extra-territorial jurisdiction.

65 The Cloud Evidence Group discussed a number of other cases, including Microsoft v. United States regarding a search warrant for an email account controlled and maintained by Microsoft on a server in Ireland. In July 2016, a US Court of Appeals rendered a decision that the US Government cannot force a company to turn over customer emails stored on servers outside the United States.[47] The Court concluded "that Congress did not intend the SCA's [Stored Communications Act's] warrant provisions to apply extraterritorially" and "that an SCA warrant may reach only data stored within United States boundaries". The decision is about the limits of specific domestic legislation but contains a number of interesting points.

66 The judgment refers to the concept of "comity":[48]

> Our conclusion today also serves the interests of comity that, as the MLAT process reflects, ordinarily govern the conduct of cross-boundary criminal investigations. Admittedly, we cannot be certain of the scope of the obligations that the laws of a foreign sovereign—and in particular, here, of Ireland or the E.U.—place on a service provider storing digital data or otherwise conducting business within its territory. But we find it difficult to dismiss those interests out of hand on the theory that the foreign sovereign's interests are unaffected when a United States judge issues an order requiring a service provider to "collect" from servers located overseas and "import" into the United States data, possibly belonging to a foreign citizen, simply because the service provider has a base of operations within the United States. Thus, to enforce the Warrant, insofar as it directs Microsoft to seize the contents of its customer's communications stored in Ireland, constitutes an unlawful extraterritorial application of the Act. [49]

[47] http://cases.justia.com/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.pdf?ts=1468508412
[48] The U.S. Supreme Court's holding in Hilton v. Guyot (1895) that the enforcement of a foreign judgment was a matter of comity is viewed as the "classic" statement of comity in international law.[14][15] The Court held in that case: "Comity," in the legal sense, is neither a matter of absolute obligation, on the one hand, nor of mere courtesy and good will, upon the other. But it is the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens or of other persons who are under the protection of its laws
[49] Page 42 http://cases.justia.com/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.pdf?ts=1468508412

67 Concurring with the judgment, Judge Gerard Lynch emphasized "the need for congressional action to revise a badly outdated statute".[50] Among other things, he added the following observation:

> Because Microsoft relies solely on customers' self-reporting in classifying customers by residence, and stores emails (but only for the most part, and only in the interests of efficiency and good customer service) on local servers – and because the government did not include in its warrant application such information, if any, as it had about the target of its investigation – we do not know the nationality of the customer. If he or she is Irish (as for all we know the customer is), the case might present a troubling prospect from an international perspective: the Irish government and the European Union would have a considerable grievance if the United States sought to obtain the emails of an Irish national, stored in Ireland, from an American company which had marketed its services to Irish customers in Ireland. The case looks rather different, however – at least to me, and I would hope to the people and officials of Ireland and the E.U. – if the American government is demanding from an American company emails of an American citizen resident in the U.S., which are accessible at the push of a button in Redmond, Washington, and which are stored on a server in Ireland only as a result of the American customer's misrepresenting his or her residence, for the purpose of facilitating domestic violations of American law, by exploiting a policy of the American company that exists solely for reasons of convenience and that could be changed, either in general or as applied to the particular customer, at the whim of the American company. Given that the extraterritoriality inquiry is essentially an effort to capture the congressional will, it seems to me that it would be remarkably formalistic to classify such a demand as an extraterritorial application of what is effectively the subpoena power of an American court.

68 With regard to the disclosure not only of subscriber information and traffic data by US service providers to foreign authorities – which is permitted under the Electronic Communications Privacy Act – but also content data, options are under discussion between the USA and the United Kingdom which would allow service providers to respond to lawful requests from foreign authorities. In July 2016, the US Department of Justice sent a legislative proposal to Congress covering the disclosure of also content data by service providers pursuant to lawful process in the foreign country if it involves communications between foreign nationals abroad and criminal activities outside the United States with no relation to the USA other than the fact that the service provider stores data in the USA.[51] Such disclosure would need to be subject to the protection of human rights in the country requesting disclosure.[52]

69 Currently, practices and procedures, as well as conditions and safeguards for access to subscriber information under domestic laws vary considerably among Parties to the Convention.[53]

70 The CEG is of the opinion that establishing a separate regime for access to subscriber information in line with Article 18 will contribute significantly to making the MLA process regarding cybercrime and electronic evidence more efficient. A Guidance Note on Article 18 with respect to subscriber information – representing the common understanding of the Parties – is needed. It would help "facilitate greater harmonisation between the Parties on the conditions, rules and procedures for obtaining subscriber information" as recommended by the T-CY already in December 2014.[54] It would allow using Article 18 more clearly as a legal basis for direct requests to service providers in other jurisdictions that are offering a service in the territory of a Party.

[50] In a letter to Congress dated 15 July 2016, the US Department of Justice stated that
[51] https://assets.documentcloud.org/documents/2994379/2016-7-15-US-UK-Biden-With-Enclosures.pdf
[52] In the cover letter, the US Department of Justice stated that it would soon send additional proposals to address the problems that had arisen in the Microsoft search warrant case.
[53] In October 2015, the T-CY Cloud Evidence Group circulated a questionnaire to Parties and Observers regarding the practical application of Article 18.1.b (see compilation of replies received in document T-CY(2015)22)
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805a0873
[54] http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7ad1

3.5 "Voluntary disclosure" by private sector entities to criminal justice authorities in foreign jurisdictions

71 Some providers may respond directly to lawful requests for subscriber information and traffic data by criminal justice authorities in other jurisdictions where they are offering a service. Service providers may also preserve data upon a preservation request received directly from a foreign criminal justice authority. The practice of voluntary disclosure is predominantly applied by US service providers as this possibility is specifically foreseen in the Electronic Communications Privacy Act.

72 The Cloud Evidence Group held two meetings with service providers in 2015 and 2016, and prepared a background study.[55]

73 The study shows that direct transborder cooperation with US service providers is practiced by more or less all Parties to the Budapest Convention, although there are considerable differences in the use of this option between Parties. For illustration, in 2014 more than 100,000 requests were sent by Parties to the Convention – other than the USA – to six major providers with a response rate of some 60%. In 2015, the number of requests increased to more than 138,000 with a similar response rate.

Direct requests for data to and voluntary disclosure in 2015	Requests to Apple, Facebook, Google, Microsoft, Twitter and Yahoo[56]		
Parties	Received	Disclosure	%
Albania	13	11	85%
Armenia	13	10	77%
Australia	6 777	4 580	68%
Austria	254	119	47%
Azerbaijan	5	-	0%
Belgium	1 992	1 453	73%
Bosnia and Herzegovina	26	8	31%
Bulgaria	8	2	25%
Canada	1 157	884	76%
Croatia	33	19	58%
Cyprus	24	4	17%
Czech Republic	431	261	61%
Denmark	342	166	49%
Dominican Republic	207	114	55%
Estonia	79	52	66%
Finland	227	172	76%
France	27 213	14 746	54%
Georgia	4	3	75%
Germany	29 092	15 469	53%
Hungary	584	214	37%

[55] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064b77d

[56] Source: Transparency reports
Apple http://www.apple.com/privacy/transparency-reports/
Facebook https://govtrequests.facebook.com/about/#
Google https://www.google.com/transparencyreport/
Microsoft https://www.microsoft.com/about/csr/transparencyhub/
Twitter https://transparency.twitter.com/
Yahoo https://transparency.yahoo.com/government-data-requests

Direct requests for data to and voluntary disclosure in 2015	Requests to Apple, Facebook, Google, Microsoft, Twitter and Yahoo[56]		
Parties	Received	Disclosure	%
Iceland	3	2	67%
Italy	7 847	3 591	46%
Japan	2 018	1 112	55%
Latvia	-	-	
Lichtenstein	7	3	43%
Lithuania	158	87	55%
Luxembourg	122	83	68%
Malta	628	338	54%
Mauritius	-	-	
Moldova	15	6	40%
Montenegro	21	10	48%
Netherlands	1 605	1 213	76%
Norway	373	234	63%
Panama	5	3	60%
Poland	2 378	820	34%
Portugal	3 255	1 751	54%
Romania	76	30	39%
Serbia	60	41	68%
Slovakia	102	29	28%
Slovenia	22	14	64%
Spain	4 151	2 092	50%
Sri Lanka	2	1	50%
Switzerland	534	267	50%
“The former Yugoslav Republic of Macedonia”	33	17	52%
Turkey	16 760	11 418	68%
Ukraine	19	5	26%
United Kingdom	29 937	21 075	70%
USA	89 350	70 116	78%
Total excluding USA	138 612	82 529	60%
Total including USA	227 962	152 644	67%

74 The study underlines the value of this cooperation, in particular by US providers:

- The European Court of Human Rights, in the case of K. U. v. Finland[57] in December 2008, confirmed the obligation of States to protect the rights of individuals, including through efficient criminal law measures. In its analysis, the Court referred to the procedural law provisions of the Budapest Convention on Cybercrime, including in particular the production of subscriber information under Article 18. It also referred to the need for efficient cooperation between service providers and law enforcement authorities as proposed in Guidelines adopted by the Council of Europe Octopus Conference in April 2008.[58]

[57] http://hudoc.echr.coe.int/eng#{"dmdocnumber":["843777"],"itemid":["001-89964"]}
[58] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3ba

- Thus, cooperation between service providers and law enforcement authorities is essential for crime prevention and criminal justice, for the strengthening of the rule of law and for the protection of human rights.

- US service providers often cooperate directly transborder with law enforcement authorities of other Parties to the Budapest Convention and disclose in particular subscriber information. The CEG is of the opinion that, in some ways, this is in line with the intent of Article 18.1.b Budapest Convention.

- In this context, a service provider having possession or control of the data cooperates with a law enforcement authority having jurisdiction over a specific offence which is being investigated. The actual location of data and servers is of limited relevance.

- Parties to the Budapest Convention – other than the USA – send more than 135,000 requests per year to major US service providers and receive (at least partial) data in about 60% of the cases.

75 While this practice of US service providers is most valuable for crime prevention and criminal justice, the CEG has a number of observations based on the aforementioned study as well as meetings with providers and data protection authorities:

- The volatility of provider policies and unpredictability of disclosure:
  Provider policies are volatile and lack foreseeability for law enforcement as well as customers. Service providers may change their policies unilaterally at any time and without prior notice to law enforcement.
  Adding to this, policies and practices not only differ widely between providers but also with respect to different Parties to the Budapest Convention. One provider may respond to many requests from one country but to none or a few requests only from another country, while the practices of another provider may be exactly the opposite.
  Given the voluntary character of the cooperation, the final decision on the disclosure of data rests with providers with a possibility of appeal.
  Overall, provider policies and practices are volatile and unpredictable which is problematic from a rule of law perspective.

- "US" versus "European" and other providers:
  While US providers are able to disclose subscriber and traffic data directly and voluntarily to foreign law enforcement authorities upon request under US law (Electronic Communications Privacy Act)[59] this is not the case for European providers. It would seem that this often due to domestic legislation (including on data retention and e-privacy) stipulating that the data must be disclosed only to the national judicial authorities in accordance with a formal procedure.[60]
  The consequence is a one-way flow of data from US service providers to the law enforcement authorities of Parties in Europe and other regions, while service providers in Europe or other Parties do not disclose data directly and voluntarily to the authorities in the US or other Parties.
  Increasingly, US service providers are represented within the European Union – for example through subsidiaries in Ireland – and are thus subject to European Union law, including data protection regulations. This may restrict possibilities for direct and voluntary transborder cooperation in the future.

[59] 18 U.S. Code §2702 https://www.law.cornell.edu/uscode/text/18/2702
[60] In Italy, for example, in the last years the most important telecommunication providers (Tim, Vodafone, Wind and H3G) received only 4 requests of data directly from European law enforcement authorities. Their response was that a MLAT had to be requested to the national judicial authority in accordance with the Italian data protection law (Legislative Decree no. 196 of 30 June 2003 – Personal Data Protection Code, section 132). http://www.garanteprivacy.it/home_en/italian-legislation

Furthermore, within the European Union, a distinction is made between Electronic Communication Service providers (which are currently subject to the confidentiality requirements of the E-Privacy Directive),[61] and Internet Society Service providers.[62]

- Location of data:

  For most US providers, the actual location of subscriber information seems to be of limited relevance.

  Conditions for access to subscriber information seem to be determined by (a) the location of the service provider and the regulations that govern the service provider, and (b) whether the requesting law enforcement authority has jurisdiction over the offence investigated. Under certain conditions, US service providers tend to disclose subscriber information to law enforcement authorities in countries where they are offering a service as foreseen in Article 18.1.b Budapest Convention. However, several major providers have self-made rules barring disclosures when an IP address resolves to a country other than the requesting country.

  European providers seem to be bound by rules of territoriality, including the location of data. The hearing held on 30 November 2015[63] suggests that for European providers this is a major obstacle to business. With regard to content data, US providers are unclear. In some instances, they may argue that content is stored in the US and thus voluntary disclosure is not possible (unless in emergency situations). In other instances, where data may be stored in Europe, they still require a mutual legal assistance request to be sent to the US Government.

- Data protection:

  The more US providers are established in Europe, the more they will be subject to European data protection rules.

  European and international data protection instruments cover transborder data transfers either from one private sector entity to another private sector entity or from one competent criminal justice authority to another criminal justice authority.

  The “asymmetric” transfer of data from a law enforcement authority of one jurisdiction to a private sector entity in another jurisdiction in another State – for example, sending an IP address to ask for the related subscriber information – is permitted under specific conditions.[64]

  However, for the “asymmetric” voluntary disclosure of data – such as subscriber information – from a private sector service provider to a law enforcement authority in another State, clear rules permitting such transfers do not seem to be available.

  Providers need to assess themselves whether the condition of lawfulness is met, whether it is in the public interest or whether it is in the legitimate interest of the provider as the data controller to disclose data. Providers may run the risk of being held liable. A clearer framework for private to public transborder disclosure of data would be required, including conditions and safeguards. This would help service providers avoid situations of conflicting legal obligations.

[61] This Directive (2002/58/EC) is currently under review https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive
[62] As defined in the E-Commerce Directive 2000/31/EC of 2000. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN
[63] http://www.coe.int/en/web/cybercrime/hearing
[64] Article 14 of Framework Decision 2008/977/JHA http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008F0977&from=EN and Article 39 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC

- Domestic legal basis for obtaining subscriber information:
  A clear basis in domestic law for production orders for subscriber information facilitates cooperation with providers. As documented in the T-CY report on rules for obtaining subscriber information[65], conditions for access to such data vary between the Parties. In some, police officers and in others prosecutors can request the production of subscriber information while in some others court orders are required. In the latter case, service providers may not respond to a request from a police or prosecution authority.
  A clear legal basis for obtaining subscriber information in domestic law, preferably harmonized in Parties, would facilitate more systematic cooperation with providers in foreign jurisdictions and use of information received in criminal proceedings.

- Direct preservation requests:
  US service providers accept requests for preservation of any data directly received from foreign authorities in the expectation that this will be followed by a request for disclosure via mutual legal assistance. However, the fact that often there is no follow up through mutual legal assistance is of concern to them.
  European providers do not accept preservation requests received directly from law enforcement authorities in other jurisdictions.

- Emergency requests:
  US service providers foresee procedures for cooperation in emergency situations, including the disclosure of contents.
  In some Parties, specific procedures have been agreed upon, including centralized systems with contact points. In these Parties, the experience seems to be positive overall, although cooperation with some providers is considered not always predictable or reliable even in emergency situations.
  It would seem that while US service providers do cooperate in principle in emergency situations, European providers do not disclose subscriber information or other data directly to foreign authorities, even in emergency situations.

- Customer notification:
  Law enforcement authorities have pointed to the practice, again differing between providers and to an unpredictable extent, of service providers notifying their clients of a request for "their" data by foreign authorities. This can adversely impact a criminal justice investigation. The notification of a customer of a request from a foreign authority by US service providers is considered a major concern by law enforcement authorities.[66]
  While confidentiality requirements may be enforced in domestic legal requests, this is less the case in situations of voluntary cooperation with a foreign provider.

- Lawful requests versus voluntary cooperation:
  A lawful order by a police, prosecutor or judge served on a physical or legal person is binding and can be enforced on the territory of the authority.
  However, under the current practice of direct transborder cooperation, US service providers consider their cooperation as "voluntary". At the same time, they frequently request to be sent an order valid in the requesting country even though it is not valid in the US.
  The current practice appears to combine a lawful, coercive request with voluntary cooperation.
  US service providers seem to prefer to keep this practice.

[65] T-CY (2014)17
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7ad1
[66] In many countries, law enforcement requests are confidential by law. Requesters from such countries may not be aware that this is not the case in the US unless they are warned.

From a law enforcement perspective this appears to be problematic as service providers determine whether or not to cooperate, evaluate the legality of the request, or check dual criminality and other conditions. This applies not only to requests for data received from police, but also prosecutors and courts; and in the end the requests are not enforceable.[67] The fact that service providers have so much discretion is problematic from a rule of law perspective.

76 The CEG thus concludes that:

- More consistent and transparent policies and operating procedures by all types of providers – for example through self-regulation or guidelines – would be desirable. Continuation of the dialogue with service providers is necessary. Regular meetings of the T-CY with service providers, the establishment of an online tool with up-to-date provider policies and procedures as well as information on relevant legislation and criminal justice authorities responsible in Parties, and common templates for requests for subscriber information may help improve current practices with respect to Parties to the Budapest Convention.

- However, it will not only be necessary to improve current practices. The establishment of clear domestic and international legal frameworks to ensure greater legal certainty for law enforcement and industry and to remove obstacles for businesses is urgently required.[68] Such a solution may be constructed around Article 18 Budapest Convention and provisions in an Additional Protocol to the Convention.

3.6 Emergency procedures

77 In exigent circumstances, emergency procedures to prevent imminent danger to life and public security would be needed to obtain electronic evidence stored in foreign jurisdictions through mutual legal assistance.

78 The T-CY in its assessment report on the mutual legal assistance provisions of the Budapest Convention[69] in December 2014, therefore, also adopted Recommendation 8 under which "Parties are encouraged to establish emergency procedures for requests related to risks of life and similar exigent circumstances. The T-CY should document practices by Parties and providers." The Cloud Evidence Group followed up on this in April/May 2016 and invited Parties to respond to a questionnaire to this effect.

79 The T-CY Cloud Evidence Group noted that US-based service providers also offer direct cooperation in emergency situations, including the production of content data.[70] The questionnaire thus not only covered emergency requests for the immediate disclosure of data through mutual legal assistance but also through direct requests to service providers.

80 Replies from 33 Parties and Observer States[71] suggest the following:

- The majority of these States (20 States or 61%) do not have legislation permitting disclosure of data by service providers to domestic criminal justice authorities in emergency situations without judicial authorisation.

[67] See in this connection the final judgement by the Belgian Court of Cassation confirming that Yahoo! is obliged to produce data upon a lawful request for data in Belgium.
http://www.lexology.com/library/detail.aspx?g=46b1a5f4-1ec4-4318-b7e9-753b23afa79f
[68] This was also the conclusion the hearing for service providers held on 30 November 2015
http://www.coe.int/en/web/cybercrime/hearing
[69] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c
[70] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064b77d
[71] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680651a6f

- From among the 13 States (39%) that can obtain data in emergency situations at the domestic level, seven can obtain all types of data including content while five can only obtain non-content data and one State only subscriber information without judicial authorisation.

- Only six out of 33 States (18%) have procedures in place to disclose data to foreign authorities in an expedited manner. One additional State referred to Article 29.7 Budapest Convention as basis for urgent cooperation even without a specific formal basis in domestic law.

- With the exception of two States (Japan and the USA), no other State has legislation permitting a service provider in its territory to disclose data to foreign law enforcement in emergency situations without mutual legal assistance.

- Major US-based service providers have established procedures for the disclosure of data in emergency situations to domestic and foreign authorities.[72] This may cover serious threats to the life/safety of individuals, the security of a State, commit substantial damage to critical infrastructure (Apple), imminent harm to a child or risk of death or serious physical injury to any person (Facebook), necessity to prevent death or serious physical harm to a person (Google, Microsoft, Twitter, Yahoo!). The disclosure is at the discretion of the service provider. They may also notify the customer either immediately or within 90 days.

- European and other providers do not seem to have emergency procedures in place and do not seem to cooperate directly with foreign authorities in emergency situations.

81 The CEG concludes that:

- Recommendation 8 of the T-CY assessment report remains to be implemented in the majority of Parties and Observer States; and the T-CY should call on Parties to do so. It may be necessary to consider a specific provision in a Protocol to the Budapest Convention to ensure greater consistency between Parties.

- Further consideration should be given to authorising service providers to respond directly to foreign requests in emergency situations as is already the case in the USA and – to some extent – Japan.

- More consistent and transparent operating procedures for disclosure of data in emergency situations by all types of providers would be desirable.

3.7 Data protection requirements

82 At present, the majority of Parties to the Budapest Convention are Parties to data protection Convention 108 of the Council of Europe[73] and about half are member States of the European Union and subject to European data protection rules.

83 Under the new EU General Data Protection Regulation, companies processing data of data subjects within the European Union,[74] are required to establish controllers within the EU and will need to follow EU data protection laws. The territorial scope of the EU framework is broad.[75]

[72] See pages 18 to 20 of https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064b77d

[73] In addition to the 47 member States of the Council of Europe, Mauritius acceded in June 2016 and Uruguay in April 2013. Cabo Verde, Morocco, Senegal and Tunisia have been invited to accede (status: 31 July 2016). http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=nopYjPBz

84 European data protection instruments are thus relevant for non-EU Parties to the Budapest Convention as they may affect their cooperation with EU member States and Parties to Convention 108.

85 Instruments currently in force include in particular:

- Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108)[76]
- Council of Europe Recommendation "R(87)15 Regulating the use of personal data in the police sector"[77]
- European Union Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data[78]
- European Union Framework Decision 2008/977/JHA of the European Union on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters[79]
- E-Privacy Directive (2002/58/EC).[80]

86 In May 2016, the European Union published in the EU Official Journal the adopted texts of two new instruments:

- The General Data Protection Regulation[81]. The GDPR will apply from 25 May 2018
- The "Police Directive"[82] which is to be transposed by EU Member States by 6 May 2018.

87 The Council of Europe is now also in the process of finalising the modernisation of its data protection Convention 108.[83]

88 Discussions with data protection organisations[84] regarding new European data protection standards suggest the following:

---

[74] See Articles 3 and 27 of the future EU Regulation.
[75] Article 3 of the future General Data Protection Regulation (GDPR) and Article 4 of current Directive 95/46/EC lay down the territorial scope of application of the EU data protection legal framework. Under Article 3 GDPR, the Regulation will apply to a processor or controller established in the EU even if the processing of data takes place outside of the EU; and it applies to the processing of personal data of data subjects who are in the EU even if the controller or processor is not established in the EU if the processing is related to the offering of goods or services to such data subjects in the EU.
[76] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108
[77] https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2196553&SecMode=1&DocId=694350&Usage=2
[78] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en
[79] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008F0977&from=EN
[80] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). The Directive was amended in 2009. The revised consolidated version is here: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:PDF
[81] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC
[82] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC
[83] In June 2016, the Ad Hoc Committee on Data Protection (CAHDATA) completed its work on the Amending Protocol and requested transmission to the Committee of Ministers. http://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/CAHDATA(2016)RAPAbr_En%20final%2027%2006%202016.pdf http://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/CAHDATA(2016)01_E.pdf

- The new EU GDPR and Directive and the modernised Convention 108 of the Council of Europe should not affect the Budapest Convention in its current form:

  - The Budapest Convention requires Parties to establish specific law enforcement powers in procedural criminal law and make them subject to conditions and safeguards. These procedural law powers represent a lawful derogation from data protection principles.
  - With regard to the international sharing of personal data between competent public authorities – in particular criminal justice authorities – the Budapest Convention with its provisions on international cooperation represents a legal basis. The mutual legal assistance process is designed to ensure that rule of law requirements are met and that the rights of individuals are protected, in particular if the data sought are to be used as evidence in criminal proceedings.

- Data protection issues arise when a criminal justice authority discloses personal data to a service provider in another jurisdiction in a specific criminal investigation. To make a request on which a provider can act, a criminal justice authority must provide at least minimal personal information (such as name or email or IP address):

  - Such "asymmetrical" disclosures from a competent public authority to a private sector entity for EU member States, would fall under the new EU Police Directive. If disclosed to a service provider within the European Union it would not be considered to represent an international transfer and the general principles laid down by the Directive would apply. In principle, this should not cause problems. In particular, such transfers would need to have a basis in domestic law. Proper implementation of Article 18 could represent such a legal basis, when the said requirements of the EU Directive are met.

  - For such disclosures of minimal personal information by a criminal justice authority within the EU to a service provider in a "third" country",[85] Chapter V of the Directive applies, according to which transfers are possible under the conditions of Article 39 regarding "transfers of personal data to recipients established in third countries". Article 39 is a derogation from the general principle laid down in Article 35(1)(b) that transfers should take place only between competent authorities. As such, it should be interpreted restrictively, that is, be used on a case by case basis, in the framework of specific investigations, when no other transfer tool can be used. It is not to serve as a legal basis for massive, repetitive and structural transfers of personal data. This derogation is without "prejudice to any bilateral or multilateral international agreement in force between Member States and third countries in the field of judicial cooperation in criminal matters and police cooperation".

    The CEG, in this context considers that:

[84] http://www.coe.int/en/web/cybercrime/exchange-of-views

[85] EU data protection rules distinguish between EU Member States, States that are considered to have an adequate level of protection and to which data can be transferred without further safeguards (from among the Parties to the Budapest Convention Iceland, Liechtenstein and Norway are considered adequate as per membership in the European Economic Area, for Canada, Israel and Switzerland adequacy decisions have been adopted, and US companies will be considered adequate following the adoption of the EU-US Privacy Shield.
http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm
http://europa.eu/rapid/press-release_IP-16-2461_en.htm
At present, adequacy decisions do not cover exchanges in the law enforcement sector. However, once the new EU Police Directive applies (from May 2018) they will also apply there.

- If a request for subscriber information containing personal information is sent by a criminal justice authority to a service provider located in another jurisdiction but offering a service in the territory of the requesting authority, Article 18.1.b could serve as the legal basis if the draft Guidance Note (see appendix) is upheld by the T-CY.
- A Protocol to the Budapest Convention could foresee further conditions for requests to service providers in third countries and thus represent an international agreement referred to in Article 39.2 EU Police Directive.

- Data protection issues also arise when a service provider established within the European Union discloses personal data directly to a criminal justice authority in another jurisdiction.[86]

  - Under EU data protection legislation, the disclosure of personal data by service providers within the EU to criminal justice authorities in another jurisdiction in the future falls under the General Data Protection Regulation.[87] If one of the situations enumerated in Article 6 of the GDPR applies, disclosure by a service provider within the EU to a criminal justice authority within the EU could be possible under data protection rules. In practice and under current rules, whether or not service providers within EU Member States disclose data directly to criminal justice authorities in other EU Member States depends on the law of the Member State implementing Directive 95/46/EC and the E-Privacy Directive.[88]

  - The disclosure of personal data by a service provider within the EU to a criminal justice authority in a third country seems to be possible by way of an adequacy decision (Article 45 GDPR), appropriate safeguards (Article 46) or derogations for specific situations (Article 49). These appear to be exceptions to Article 44 (General prohibition of international transfers outside of the EU) and are therefore subject to restrictive interpretation. Furthermore, Article 48 on transfers or disclosures not authorized by Union law refers to international agreements as a potential basis for the transfer or disclosure of data to an authority in a third country upon a lawful request.

    The CEG, in this context considers that:

    - If subscriber information is disclosed by a service provider to a criminal justice authority in another jurisdiction upon a production order, Article 18.1.b could serve as the legal basis if the service provider is offering a service in the territory of the requesting authority, if the draft Guidance Note (see appendix) is upheld by the T-CY.

[86] In the exchange of views on 23 May 2016, some participants raised possible concerns in relation to Article 32 (transborder access to data) and the question of whether a service provider could consent to disclose data under this provision. However, others pointed at the Guidance Note on Article 32b which states that "Service providers are unlikely to be able to consent validly and voluntarily to disclosure of their users' data under Article 32".
http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726a
[87] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
[88] For example, the disclosure of data to foreign authorities by Facebook Ireland is considered compatible with Irish data protection legislation. In 2011 and 2012, Facebook Ireland was audited by the Irish Data Protection Commissioner, including with respect to disclosure to foreign authorities.
See Section 3.7 (page 98 ff) and appendix 5 in the report of 2011
https://www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf
See Section 2.7 (page 34 ff) in the report of 2012
https://www.dataprotection.ie/docs/21-09-12-Facebook-Ireland-Audit-Review-Report/1232.htm

  - A Protocol to the Budapest Convention could foresee further provisions regarding the disclosure of subscriber information to a criminal justice authority in a third country.

- The practice of US service providers to notify customers of lawful requests for data is of major concern to criminal justice authorities as it may compromise investigations and create risks to investigators, prosecutors and others. Customer notification is not a general requirement under European data protection rules. Confidentiality requirements may be imposed under domestic law, and appear to be foreseen in the criminal procedure laws of most European countries.

4 Solutions

89 The Cloud Evidence Group – taking into account previous work of the Cybercrime Convention Committee on mutual legal assistance, subscriber information, transborder access to data and other topics as well as other relevant international and European developments – is proposing to the T-CY a combination of solutions for consideration. They are not meant as alternatives but should be pursued in parallel.

4.1 Legal and practical measures at domestic levels to render mutual legal assistance more efficient (Recommendations 1 – 15 of the T-CY assessment report on MLA)[89]

90 The CEG concludes that mutual legal assistance remains the main means to obtain electronic evidence from foreign jurisdictions for use in domestic criminal proceedings. This is particularly true for content data.

91 The Cloud Evidence Group is of the view that while mutual legal assistance is often not feasible in the context of cloud computing, the possibilities of the mutual legal assistance process should be exhausted. Otherwise, new and innovative approaches would not find broad acceptance.

92 Parties should, therefore, give follow up to those Recommendations adopted by the T-CY in December 2014 falling primarily under the responsibility of domestic authorities:

Rec 1 Parties should fully implement and apply the provisions of the Budapest Convention on Cybercrime, including preservation powers (follow up to T-CY Assessment Report 2012).

Rec 2 Parties should consider maintaining statistics or establish other mechanisms to monitor the efficiency of the mutual legal assistance process related to cybercrime and electronic evidence.

Rec 3 Parties should consider allocating more and more technology-literate staff for mutual legal assistance not only at central levels but also at the level of institutions responsible for executing requests (such as local prosecution offices).

Rec 4 Parties should consider providing for better training to enhance mutual legal assistance, police-to-police and other forms of international cooperation on cybercrime and electronic evidence. Training and experience exchange should in particular target prosecutors and judges and encourage direct cooperation between judicial authorities. Such training should be supported by the capacity building programmes of the Council of Europe and other organisations.

Rec 5 Parties and the Council of Europe should work toward strengthening the role of 24/7 points of contact in line with Article 35 Budapest Convention, including through:

a. Ensuring, pursuant to article 35.3 Budapest Convention that trained and equipped personnel is available to facilitate the operative work and conduct or support mutual legal assistance (MLA) activities
b. Encouraging contact points to pro-actively promote their role among domestic and foreign counterpart authorities;
c. Conducting regular meetings and training of the 24/7 network among the Parties;
d. Encouraging competent authorities and 24/7 points of contact to consider procedures to follow up to and provide feedback to the requesting State on Article 31 requests;

[89] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c

e. Considering to establish, where feasible, contact points in prosecution offices to permit a more direct role in mutual legal assistance and a quicker response to requests;
f. Facilitating 24/7 points of contact to play a supportive role in "Article 31" requests.

Rec 6 Parties should consider streamlining the procedures and reduce the number of steps required for mutual assistance requests at the domestic level. Parties should share good practices in this respect with the T-CY.

Rec 7 Parties should make use of all available channels for international cooperation. This may include formal mutual legal assistance, police to police cooperation and others.

Rec 8 Parties are encouraged to establish emergency procedures for requests related to risks of life and similar exigent circumstances. The T-CY should document practices by Parties and providers.

Rec 9 Parties should confirm receipt of requests systematically and give, upon request, notice of action taken.

Rec 10 Parties may consider the opening of domestic investigation upon a foreign request or spontaneous information to facilitate the sharing of information or accelerate MLA.

Rec 11 Parties should make use of electronic transmission of requests in line with Article 25.3 Budapest Convention on expedited means of communication.

Rec 12 Parties should ensure that requests are specific and complete with all necessary information.

Rec 13 Pursuant to Article 25.5 Budapest Convention and Paragraph 259 Explanatory Report, Parties are reminded to apply the dual criminality standard in a flexible manner that will facilitate the granting of assistance.

Rec 14 Parties are encouraged to consult with authorities of requested Party prior to sending requests, when necessary.

Rec 15 Parties should consider ensuring transparency regarding requirements for mutual assistance requests, and reasons for refusal, including thresholds for minor cases, on the websites of central authorities.

93 Recommendation 8 on emergency procedures may also need to be addressed in a Protocol to the Budapest Convention.

94 The T-CY should review follow up given by Parties to Recommendations 1 to 15 in detail.

95 The Council of Europe – through capacity building projects – should support implementation of Recommendations 1 to 15 if necessary, and follow up on Recommendations 17 and 18:

Rec 17 The Council of Europe should – under capacity building projects – develop or link to standardised, multi-language templates for Article 31-requests.

Rec 18 The Council of Europe should explore the possibility of establishing an online resource providing information on laws of Parties on electronic evidence and cybercrime as well as on legal thresholds, and evidentiary and other requirements to be met to obtain the disclosure of stored computer data for use in court proceedings.

4.2 Guidance Note on Article 18 Budapest Convention on obtaining of subscriber information and clarification of when a service provider is within the jurisdiction of a criminal justice authority

96 The CEG recommends that the T-CY consider adoption of a Guidance Note to address the question of production orders for subscriber information under Article 18, that is, situations in which:

- a person ordered to produce specified computer data is present in the territory of a Party (Article 18.1.a);[90]
- a service provider ordered to produce subscriber information is offering a service in the territory of the Party without necessarily being located in the territory (Article 18.1.b).

97 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 located 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 enforceability of domestic production orders outside the territory of a Party raises further issues.

98 Such a Guidance Note would help States make better use of orders for the production of subscriber information from service providers in the territory or offering a service in the territory of a Party under Article 18 Budapest Convention. Considering the challenges of cloud computing, better use of this provision in the sense proposed would be an efficient and lawful means to obtain the type of information needed most often in a criminal investigation.

99 A common understanding of Article 18 with respect to subscriber information as proposed in the attached Guidance Note would also allow considering Article 18 as a legal basis for the current practice of direct requests for subscriber information to service providers in foreign jurisdictions.

100 A draft Guidance Note is appended to this report for consideration by the T-CY.

[90] 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. The proposed Guidance Note, however, addresses the production of subscriber information only.

4.3 Domestic rules and procedures on access to subscriber information

101 Parties should facilitate access to subscriber information in domestic legislation by differentiating between traffic data and subscriber information and thus by fully implementing Article 18 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.

102 As subscriber information is less privacy sensitive than traffic data and content data, conditions for production orders for subscriber information should be subject to lesser safeguards than for other types of data or for other types of intrusive powers.

103 A lighter regime for the production of subscriber information will facilitate domestic investigations and international cooperation in a cloud context.

4.4 Practical measures to facilitate transborder cooperation between service providers and criminal justice authorities

104 Pending longer-term solutions, practical measures could be taken to facilitate more coherent cooperation between service providers and criminal justice authorities, in particular with respect to the disclosure of subscriber information upon a lawful request in a specific criminal investigation but also with respect to emergency situations, and by referring to legitimate interests and applicable data protection requirements.

105 To this effect the CEG suggests that:

- the T-CY should consider an annual meeting with service providers back-to-back with a T-CY Plenary in order to promote more consistent and transparent policies and operating procedures by all types of providers;
- the Council of Europe (T-CY Secretariat and capacity building projects) should establish and maintain an online resource on provider policies and on procedural rules in Parties regarding production orders for subscriber information. Parties should ensure that the information regarding their rules and procedures is accurate and up-to-date;
- the Cybercrime Programme Office of the Council of Europe should involve service providers capacity building projects to facilitate law enforcement/service provider cooperation and call on service providers to provide training in the use of their procedures;
- The T-CY could liaise with the EU Commission so that both organisations are kept informed of each other's work and that synergies are ensured.

4.5 Additional Protocol to the Budapest Convention

106 The Cloud Evidence Group recommends starting negotiation of an additional Protocol to the Budapest Convention on Cybercrime in order to allow for more effective mutual legal assistance, to facilitate direct cooperation with service providers in other jurisdictions when needed and subject to conditions and safeguards, to frame and establish conditions and safeguards regarding existing practices of transborder access to data and to establish data protection requirements.

107 It is recalled, in this connection, that the Parliamentary Assembly of the Council of Europe – in Recommendation 2077 (2015)[91] on "Increasing co-operation against cyberterrorism and other large-scale attacks on the Internet" invited the Parties to the Convention on Cybercrime, among other things, to study the feasibility of an Additional Protocol regarding criminal justice access to data on cloud servers as well as regarding transborder access to data by extending the scope of Article 32 Budapest Convention.

108 The following are elements for reflection. Their feasibility would need to be determined during the negotiation of a Protocol. Other elements may also be considered in the course of the process.

4.5.1 Provisions for more effective mutual legal assistance

109 The T-CY Assessment Report on the functioning of mutual legal assistance[92] adopted by the T-CY in December 2014 contains Recommendations which are to be addressed through a Protocol to the Budapest Convention. Those Recommendations remain valid.

4.5.1.1 A simplified regime for mutual legal assistance requests for subscriber information (Rec 19 T-CY Assessment Report)

110 Recommendation 19 of the T-CY Assessment Report on mutual legal assistance states:

> Parties should consider allowing - via legal domestic amendments and international agreement - for the expedited disclosure of the identity and physical address of the subscriber of a specific IP address or user account.

111 While Article 18 Budapest Convention is a domestic power for the production of data (Article 18.1.a) by a person in the territory or of subscriber information by a service provider offering a service in the territory (18.1.b) other situations may arise where Article 18 as a domestic power is not applicable or cannot be enforced.

112 Article 31 Budapest Convention on mutual assistance regarding accessing of stored computer data requires that requests "shall be responded to on an expedited basis". However, Article 31 does not differentiate between types of data and does not provide a mechanism for expedited disclosure of data.

113 Given the need for subscriber information often at an early stage of an investigation and given that subscriber information is less privacy sensitive than traffic or content data, a Protocol could establish a simplified mutual legal assistance regime ensuring expedited responses to requests for subscriber information.

114 Such a regime could complement Article 18 with respect to subscriber information, including in situations where a service provider refuses to respond to domestic production orders from competent authorities of a Party where the service provider is offering a service (Article 18.1.b).

[91] http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21976&lang=en
[92] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c

4.5.1.2 International production orders (Rec 20 T-CY Assessment Report)

115 Recommendation 20 of the T-CY Assessment Report on mutual legal assistance states:

> Interested Parties may consider the possibility and scope of an international production order to be directly sent by the authorities of a Party to the law enforcement authorities of another Party.

116 The T-CY in this connection may draw on Directive 2014/41/EU on the European Investigation Order (EIO)[93] which is an order to be issued by the authorities of one EU Member State and recognized and executed by the authorities of another EU Member State.

> (7) An EIO is to be issued for the purpose of having one or several specific investigative measure(s) carried out in the State executing the EIO ('the executing State') with a view to gathering evidence. This includes the obtaining of evidence that is already in the possession of the executing authority.

117 The EIO Directive "establishes a single regime for obtaining evidence". It is not specific to electronic evidence. However, the Justice and Home Affairs Council of the EU, in its "Council conclusions on improving criminal justice in cyberspace" adopted on 9 June 2016[94] underlines the value of the EIO to secure electronic evidence within the European Union. It calls on EU Member States to "swiftly transpose the EIO Directive", and:

> The COMMISSION is requested, with a view to making full use of Directive 2014/41/EU on the European Investigation Order in Criminal Matters ("the EIO Directive") for the purposes of securing and obtaining e-evidence in the EU, to continue monitoring and supporting Member States in the transposition process of this directive by 22 May 2017.

118 When preparing a draft Protocol to the Budapest Convention, the feasibility of incorporating elements of the EIO into a Protocol as an international production order could be established.

4.5.1.3 Direct cooperation between judicial authorities in mutual legal assistance requests (Rec 21 T-CY Assessment Report)

119 Recommendation 21 of the T-CY Assessment Report on mutual legal assistance states:

> Parties should consider enhancing direct cooperation between judicial authorities in mutual legal assistance requests.

120 The T-CY Assessment Report on mutual legal assistance with regard to channels and means of cooperation concluded inter alia:

> Concl 11: Most Parties make use of different bilateral, regional and multilateral agreements or the principle of reciprocity, and multiple authorities and channels of cooperation as foreseen in the Budapest Convention on Cybercrime. Some States, however, follow a more limited approach and require MLA requests to be sent via Ministries of Justice and a few only accept requests via diplomatic channels.
>
> Concl 12: The possibility of direct cooperation with foreign judicial authorities appears to be underused – except between EU member States. This limited use of the option of direct cooperation also seems to be the case for non-EU States that are nevertheless Parties to the

[93] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0041&from=EN
[94] http://www.consilium.europa.eu/en/press/press-releases/2016/06/09-criminal-activities-cyberspace/

> 2nd Additional Protocol to the Convention on Mutual Legal Assistance in Criminal Matters (ETS 182) of the Council of Europe. It may be worth considering provisions allowing for direct cooperation between Parties to the Budapest Convention.

121 The Budapest Convention, in Article 25.3, refers to expedited technical means of cooperation and in Article 27.1.b to direct communication between designated central authorities.

122 However, other instruments on mutual legal assistance offer the possibility of forwarding requests directly from one judicial authority of a requesting Party to a judicial authority of a requested Party. This is the case of Article 4 of the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS 182)[95] of the Council of Europe or of Article 6 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.[96]

123 A similar provision could be foreseen in a Protocol to the Budapest Convention to make this option also available to Parties that are not Parties to such treaties.

4.5.1.4 Joint investigations and joint investigation teams (Rec 23 T-CY Assessment Report)

124 Recommendation 23 of the T-CY Assessment Report on mutual legal assistance states:

> Parties should consider joint investigations and/or the establishment of joint investigation teams between Parties.

125 Joint investigations or joint investigative teams can be an effective means for investigating transnational cases of cybercrime. While a specific provision to this effect is absent in the Budapest Convention, the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS 182)[97] with Article 20 comprises a detailed provision on joint investigation teams. This Article reproduces almost entirely Article 13 of the EU Convention on Mutual Assistance in Criminal Matters.

126 A provision similar to Article 20 of ETS 182 could be foreseen in a Protocol to the Budapest Convention to make this option also available to Parties that are not Parties to this treaty.

4.5.1.5 Requests in English language (Rec 24 T-CY Assessment Report)

127 Recommendation 24 of the T-CY Assessment Report on mutual legal assistance states:

> Parties should consider allowing for requests to be sent in English language. Parties should in particular be allowing for preservation requests to be sent in English.

128 The T-CY Assessment Report on mutual legal assistance stressed that:

> The question of language of international requests for mutual assistance is considered a major problem by most States. The main problems in this respect are:
>
> - delays caused by translations;
> - the cost of translations;
> - the limited quality of translations, including unclear terminology;
> - limited foreign language skills of practitioners.

[95] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/182
[96] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2000:197:0001:0023:EN:PDF
[97] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/182

> Even if for domestic purposes (legal and practical reasons) certified translations would still be required, most States accept a request in English.
>
> ...
>
> An additional Protocol to the Budapest Convention could stipulate that mutual assistance requests sent in English are accepted by the Parties, at least in urgent cases.

129 Some Parties do not accept requests in English unless this is foreseen in an international agreement to which they are Party. However, the Budapest Convention is silent with respect to the language of requests.

130 A provision allowing for requests to be sent in English language could be foreseen in a Protocol to the Budapest Convention, at least with regard to preservation requests as well as requests for subscriber information.

4.5.1.6 Audio/video hearing of witnesses, victims and experts

131 Cybercrime and other cases involving electronic evidence often involve victims and witnesses, including experts, in multiple jurisdictions and this raises major obstacles to criminal proceedings.

132 A number of international instruments, therefore, comprise provisions allowing for hearings by video or telephone conferences. An example is Articles 9 and 10 of the Second Additional Protocol to the Convention on Mutual Legal Assistance of the Council of Europe (ETS 182).[98]

133 A provision similar to Articles 9 and 10 ETS 182 could be foreseen in a Protocol to the Budapest Convention to make this option also available to Parties of the Budapest Convention that are not Parties to this treaty.

4.5.1.7 Emergency procedures (Rec 8 T-CY Assessment Report)

134 Recommendation 8 of the T-CY Assessment Report on mutual legal assistance states:

> Parties are encouraged to establish emergency procedures for requests related to risks of life and similar exigent circumstances. The T-CY should document practices by Parties and providers.

135 The Report listed this recommendation as “falling primarily under the responsibility of domestic authorities”.

136 A survey conducted by the Cloud Evidence Group[99] in Spring 2016, in which 33 States participated, shows that:

- the majority of Parties do not have legislation in place permitting disclosure of data to domestic criminal justice authorities in emergency situations;
- less than 20% have procedures in place permitting domestic competent authorities to disclose data to foreign authorities in an expedited manner;
- only two Parties permitted service providers in their territory to disclose data to foreign competent authorities in emergency situation.

[98] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/182

[99] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680651a6f

137 In the light of this and in order to ensure a consistent approach between Parties, the Cloud Evidence Group proposes to address Recommendation 8 also through a Protocol to the Budapest Convention.

4.5.2 Provisions allowing for direct cooperation with service providers in other jurisdictions

138 The Cloud Evidence Group considers that Article 18 Budapest Convention in the meaning of the proposed Guidance Note already permits the sending of production orders for subscriber information to service providers offering a service in the territory of a Party but located in another jurisdiction. Corresponding implementation of Article 18 in domestic law should make data received from service providers admissible as evidence in criminal proceedings.

139 A Protocol to the Budapest Convention may:

- clarify the procedures and conditions for such direct cooperation with service providers in other jurisdictions, and the admissibility of data received in criminal proceedings;
- establish a legal basis for direct preservation requests to foreign service providers. This is already a practice accepted by US service providers;
- provide for emergency procedures permitting direct cooperation with service providers in foreign jurisdictions in specific exigent situations.

4.5.3 Clearer framework and stronger safeguards for existing practices of transborder access to data[100]

140 The options and recommendations presented in this report so far are aimed at more efficient cooperation between criminal justice authorities and at more efficient cooperation with service providers.

141 They do not address the type of "loss of (knowledge) of location"[101] situations where multiple providers and jurisdictions may be involved or where it is not known or not feasible to identify from where an attack is originating.

142 The T-CY's Transborder Group between 2012 and 2014 determined that current international options – in particular Article 32b – offer only very limited possibilities. It noticed that in the absence of a clear and feasible international legal framework, governments increasingly pursue unilateral solutions with risks for State-to-State relations and the rights of individuals.[102]

143 The Transborder Group made a number of proposals for additional options to be considered in a Protocol to the Budapest Convention. However, in December 2014, the Group concluded that:

- in the then context negotiation of a Protocol on transborder access to data would not be feasible;
- the problems identified will not disappear but rather increase;

[100] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e70b6
[101] See for example Sansom, Gareth (2008) about the problem of "location" in cyberspace. http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/T-CY/Gareth%20Samson%20Website%20Location.pdf
[102] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726e

- 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.

144 The Cloud Evidence Group recommends some of the proposals made be reviewed again when negotiating a Protocol to the Budapest Convention:[103]

- Transborder access without consent but with lawfully obtained credentials. Such a provision could permit a Party, without the authorisation of another Party to access or receive, during a criminal investigation or trial, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the credentials by lawful investigative activities. The investigating Party would be obliged to notify the other Party, prior, during or after acquiring the data. Additional conditions and safeguards would need to be established.[104]

- Transborder access without consent in good faith or in exigent or other circumstances. Such a provision could permit transborder access in specific situations to prevent imminent danger, physical harm, the escape of a suspect or similar. Situations may also comprise the risk of destruction of relevant evidence. Again, specific criteria and safeguards as well as notification of the other Party would need to be defined. It may also need to cover "good faith" situations, where during a search, a law enforcement authority may not know (for sure) that the system searched is located on a foreign territory, or may not know on which territory, or may have obtained evidence from a foreign territory by mistake or accident. Specific conditions and safeguards would need to be established.

- The "power of disposal" or the "person in possession or control" as the connecting legal factor.[105] In "loss of (knowledge) of location" situations where data are "somewhere in the clouds", may move between different servers and locations, be split over different locations or be dynamically composed from subsets of data from different locations, or mirrored and cached and thus be available in different locations at the same time, or a person may be "in roaming" when data is accessed or intercepted, it is problematic to rely on the principle of territoriality (defined by the location of the data or computer system) to determine the jurisdiction to enforce a search or seizure of electronic evidence. It has been argued, therefore, that an approach beyond territoriality was required. A connecting legal factor that provides an alternative to territoriality could be the "power of disposal" or "the person in possession or control". Even if the location of data cannot be clearly determined, data can be connected to a person having the power to "alter, delete, suppress or to render unusable as well as the right to exclude others

[103] In 2015, the Parliamentary Assembly of the Council of Europe adopted Recommendation 2077 (2015) on "Increasing co-operation against cyberterrorism and other large-scale attacks on the Internet" which recommends to extend the scope of Article 32 of the Budapest Convention through an additional Protocol. http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=21976
In response, the Committee of Ministers of the Council of Europe noted that "the T-CY will follow developments and reconsider the feasibility of a protocol on the specific question of transborder access to data in the future". And that "the Committee of Ministers intends to follow this issue and will keep the Assembly informed about any developments in this respect."

[104] For example, this option could be limited to scenarios where access credentials have been lawfully obtained by law enforcement authorities of the searching Party, and thus avoid "hacking" by law enforcement into computer systems located in other Parties.

[105] Spoenle, Jan (2010): "Cloud computing and cybercrime investigations: territoriality vs the power of disposal", discussion paper, Project on Cybercrime, Council of Europe, Strasbourg.
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3df
See also Sansom, Gareth (2008) about the problem of "location" in cyberspace.
http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/T-CY/Gareth%20Samson%20Website%20Location.pdf

from access and any usage whatsoever".[106] Specific conditions and safeguards would need to be established.

4.5.4 Safeguards, including data protection requirements

145 Some of the measures proposed for consideration in a Protocol to the Budapest Convention may require specific conditions and safeguards, including provisions for the protection of personal data.

146 Operational agreement concluded between EUROPOL and a number of non-EU countries may serve as a source of inspiration.[107] They typically cover:

- Purpose limitation;
- Necessity of transmission of personal data;
- Limitations to onward transmission;
- Right of access to data;
- Data quality and assessment of the source and of the information;
- Storage, review, correction and deletion of personal data;
- Data security.

147 With regard to direct cooperation between criminal justice authorities of one Party with a service provider in another jurisdiction, a Protocol may need to establish specific conditions for transfers of data:

- from a criminal justice authority to a private sector entity in another jurisdiction;[108]
- from a private sector entity to a criminal justice authority in another jurisdiction.

[106] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3df

[107] https://www.europol.europa.eu/content/page/external-cooperation-31

[108] See Article 39 of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC

5 Recommendations to the T-CY

148 The Cloud Evidence Group is of the opinion that the combination of solutions proposed represents a feasible response to some of the challenges of cloud computing that criminal justice authorities are confronted with. It thus submits the following recommendations to the T-CY:

Rec 1 To invite Parties and Observer States to ensure follow up to the T-CY Recommendations on MLA adopted in December 2014 and falling primarily under the responsibility of domestic authorities, that is, Recommendations 1 to 15.[109] The T-CY to assess progress made, and capacity building programmes, if necessary, to support implementation.

Rec 2 To consider the draft Guidance Note on Production Orders for Subscriber Information as appended to this report in view of adoption and in view of offering guidance to Parties in the implementation of Article 18.

Rec 3 To invite Parties and Observer States to review domestic procedures for access to subscriber information and thus to ensure full implementation of Article 18 Budapest Convention.

Rec 4 To take practical measures – pending longer-term solutions – to facilitate more coherent cooperation between service providers and criminal justice authorities, in particular with respect to the disclosure of subscriber information upon a lawful request in a specific criminal investigation but also with respect to emergency situations.

Rec 5 To consider the preparation of a draft Protocol to the Budapest Convention with the following elements:

- Provisions for more effective mutual legal assistance
  - a simplified regime for mutual legal assistance requests for subscriber information;
  - international production orders;
  - direct cooperation between judicial authorities in mutual legal assistance requests;
  - joint investigations and joint investigation teams;
  - requests in English language;
  - audio/video hearing of witnesses, victims and experts;
  - emergency MLA procedures.

- Provisions allowing for direct cooperation with service providers in other jurisdictions with regard to requests for subscriber information, preservation requests, and emergency requests.

- Clearer framework and stronger safeguards for existing practices of transborder access to data.

- Safeguards, including data protection requirements.

In order to facilitate a formal T-CY decision by June 2017 on initiating the drafting of a Protocol, the T-CY may consider extending the mandate of the Cloud Evidence Group and request the CEG to submit draft Terms of Reference for the drafting process and additional information on possible elements to the T-CY in spring 2017.

[109] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c

6 Appendix

6.1 Cloud Evidence Group: Terms of Reference

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[110] 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[111] • Up to 5 additional members with defrayal of cost[112] • Additional T-CY members (State Parties) at their own cost.

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

6.2 (Draft) Guidance Note on "production orders for subscriber information" under Article 18 Budapest Convention

www.coe.int/TCY

Strasbourg, 14 September 2016 T-CY(2015)16

Cybercrime Convention Committee (T-CY)

T-CY Guidance Note #10 (DRAFT)

Production orders for subscriber information

(Article 18 Budapest Convention)

Proposal prepared by the T-CY Bureau and Cloud Evidence Group on 12-14 September 2016 for consideration by the T-CY

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.[113]

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

The present Note[114] addresses the question of production orders for subscriber information under Article 18, that is, situations in which:

- a person ordered to produce specified computer data is present in the territory of a Party (Article 18.1.a);[115]
- a service provider ordered to produce subscriber information is offering a service 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 enforceability of domestic production orders against providers established outside the territory of a Party raises further issues.

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 served in specific cases with regard to specified subscribers.

[113] See the mandate of the T-CY (Article 46 Budapest Convention).
[114] This Guidance Note is based on the work of the T-CY Cloud Evidence Group.
[115] 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[116]

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.[117]

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

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

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.

Obtaining subscriber information represents 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 present in the territory or offering a service in the territory of the Party.[118]

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 physically present or legally present in the Party's territory.
- With respect to computer data, the scope is broad but not indiscriminate: any "specified" computer data (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 control.
- 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/granted.

[118] 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.

3.2 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;"[119]
- is restricted to "subscriber information;"
- the service provider which is served the order is not necessarily physically present, but the service is offered in the territory and the service provider may thus be considered to be established 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 in line with Article 22 Budapest Convention. [120]

This may typically include situations in which the subscriber is or was resident or present on 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.

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".[121]

The Explanatory Report (paragraph 171) 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 which may serve as an appropriate legal basis for cooperation with service providers.

---

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

[120] Article 22 – Jurisdiction

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:
   a in its territory; or
   b on board a ship flying the flag of that Party; or
   c on board an aircraft registered under the laws of that Party; or
   d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.
2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.
3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.
4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.
5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

[121] Paragraph 172 Explanatory Report.

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. 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."[122]

- 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)."[123]

This includes situations in which the storage facility is located outside of its territory.

Regarding Article 18.1.b, a typical situation may include a service provider that has its headquarters in one jurisdiction, applies the legal regime of a second jurisdiction, and stores the data in a third jurisdiction. Data may 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 recognize, both in the criminal justice sphere and in the privacy and data protection sphere, that the location of the data is not the determining factor for establishing jurisdiction.

3.6 What is "offering a service 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 is thus subject to 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.

The T-CY has determined that with regard to Article 18.1.b, a service provider is "offering a service in the territory of the Party", when:

- 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

- orients its activities toward such subscribers (for example, by providing local advertising or advertising in the language of the territory of the Party), or makes use of the subscriber information (or associated traffic data) in the course of its activities, or interacts with subscribers in the Party.

3.7 General considerations and safeguards

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.

> Article 15.3 - 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.

[122] Paragraph 173 Explanatory Report. A "person" in Article 18.1.a Budapest Convention may be a physical or legal person, including a service provider.
[123] Paragraph 173 Explanatory Report.

3.8 Applying Article 18 with respect to subscriber information

The production of subscriber information under Article 18 Budapest Convention may, 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 in line with Article 22 Budapest Convention;</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 service provider is physically or legally present or represented in the territory of the Party. For example, the service provider is registered as a provider of electronic communication services, or servers or parts of its infrastructure are located in the Party.</td><td>OR</td><td>Article 18.1.b
The service provider is “offering a service in the territory of the Party”, that is:
- the service provider enables persons in the territory of the Party to subscribe to its services,[124] AND
- orients its activities at subscribers, or makes use of subscriber information in the course of its activities, or interacts with subscribers in the Party; AND
- the subscriber information to be produced 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.

[124] 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.”

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. _____