COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Strasbourg, version 18 February 2016

T-CY (2015)22
RESTRICTED

Cybercrime Convention Committee (T-CY)

Cloud Evidence Group

Application of Article 18.1.b Budapest Convention on "production order":

Compilation of replies to the questionnaire

Contents

Contact

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

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

Background

The T-CY in December 2014 established the "Cloud Evidence Group" tasked to explore solutions on criminal justice access to evidence stored on servers in the cloud and in foreign jurisdictions, including through mutual legal assistance.

In June 2015, the Cloud Evidence Group submitted to the T-CY a discussion paper on "Challenges".

On 30 November 2015, that is, prior to the 14th Plenary of the T-CY (1-2 December), the Group will hold a hearing for service providers. The hearing is to focus on the following specific issues:

- When is a service provider considered to be "offering a service on the territory" of a Party in the sense of Article 18.1.b Budapest Convention? And thus, when is a service provider subject to a domestic production order for subscriber information?

- Are, and if so, when do service providers respond directly to requests from foreign criminal justice authorities? What are their policies, practices, conditions and specific format and requirements for responding directly to a request for (a) subscriber, (b) traffic, and (c) content data? What are their policies, practices and procedures regarding criminal or non-criminal emergency requests?

The Cloud Evidence Group, in its meeting on 27 and 28 September 2015, came to the conclusion that in order to obtain a full understanding of these issues, Parties and Observer States are invited to share the experience and practices of their criminal justice authorities.

Parties and Observer States were invited to submit their responses by 10 November 2015.

The present document represents a compilation of the replies received.

REPLIES RECEIVED

PARTIES	**DATE**
Albania	
Armenia	
Australia	12 November 2015
Austria	
Azerbaijan	
Belgium	
Bosnia and Herzegovina	16 November 2015
Bulgaria	12 November 2015
Canada	08 February 2016
Croatia	09 November 2015
Cyprus	
Czech Republic	13 November 2015
Denmark	
Dominican Republic	
Estonia	
Finland	10 November 2015
France	12 November 2015
Georgia	
Germany	05 November 2015
Hungary	17 November 2015
Iceland	
Italy	18 January 2016
Japan	10 November 2015
Latvia	19 October 2015
Lithuania	26 November 2015
Luxembourg	29 October 2015
Malta	
Mauritius	17 November 2015
Moldova	13 October 2015
Montenegro	10 November 2015
Netherlands	08 November 2015
Norway	
Panama	
Poland	
Portugal	8 October 2015
Romania	12 November 2015
Serbia	
Slovakia	10 November 2015
Slovenia	10 November 2015
Spain	15 January 2016
Sri Lanka	
Switzerland	22 December 2015
The former Yugoslav Republic of Macedonia	
Turkey	05 November 2015
Ukraine	
United Kingdom	
United States	03 November 2015
TOTAL	**27**

OBSERVERS	**DATE**
Andorra	
Argentina	
Chile	
Colombia	
Costa Rica	
Greece	
Ireland	
Israel	
Lichtenstein	
Mexico	
Monaco	2 November 2015
Morocco	
Paraguay	
Peru	
Philippines	29 October 2015
Senegal	
South Africa	
Sweden	
Tonga	18 January 2016
TOTAL	**3**

Compilation of replies

Q 1. Domestic production orders for subscriber information when "offering a service on the territory" of a Party

Considering Article 18 paragraph 1.b. of the Budapest Convention and its explanatory report (see appendix):

a. When do you, as a criminal justice authority, consider that service provider1 is offering a service on your territory?

Australia	The *Telecommunications (Interception and Access) Act 1979* (the TIA Act), as recently amended by the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*, applies to a service if the service provider operating the service owns or operates, in Australia, infrastructure that facilitates, or relates to, the provision of any of its services. For example, if a service provider provides the telephone service equipment (i.e handset, SIM), the network or if the service provider's data is stored on servers in Australia then this would be considered to be on Australian territory and the TIA Act would apply. Under the TIA Act, service providers are now obliged to retain certain telecommunications data (including subscriber information) for a period of two years.
Bosnia and Herzegovina	**Brcko District of Bosnia and Herzegovina- The District Police - Crime Investigations Police** We consider that a service provider is offering its services on our territory either when the subscribers have their temporary/permanent residence addresses registered on the territory of our competence(it being the territory of the BiH Brcko District and of Bosnia and Herzegovina) or when a service provider is situated on the territory within our authorities **Regulatory Agency for communication** We will consider that a service provider "offers the services on the territory" of a Party in one of the following cases: - Server for storing data is not placed on the territory of the Party but the service is technically available on the territory of the Party, and the Provider did not exclude the territory of the Party by an explicit declaration when it comes to the providing services to the user within the competency of the Party; - The storing is executed on the Server which is based on the territory of the Party, in any case and regardless if the provider of the services if the legal company registered for business on the territory of the Party or storing data on the server which is based on the territory of the Party based on some other grounds; - In each particular case, regardless of the fact where is the data stored, if the

[1] The Budapest Convention applies a broad concept covering all types of service providers:

Article 1 – Definitions

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.

	stored data could be linked with the activities sanctioned by the international legal instruments which explicitly order the Party to act for the purpose of preventing the planning or executing the acts, or to remove the consequences of the acts sanctioned by the international legal order. **Federal Ministry of Internal Affairs - Federal Police Administration** The Service Provider offers services on our territory 2when they use the blocks of the IP address which are delivered to our service provider on our territory. i.e. when the data is physically stored in the media on our territory;
Bulgaria	If a legal entity is registered with the Commission on Electronic Communication as an enterprise providing electronic communications services it can be considered as a service provider.
Canada	The answer as to when a criminal justice authority in Canada considers a "service provider" to be offering a service in the territory of Canada depends on the intended scope of the term "service provider." Historically, "service provider" was often associated with firms that own or operate physical infrastructure in Canada and offer telecommunications or internet access services to people in Canada. It is straightforward to use a production order to obtain subscriber information held by these types of service providers and such service providers are clearly offering a service on our territory. The concept of "service provider" as defined in Article 1 of the Budapest Convention is quite broad, however, and does not have a direct correlate in Canadian law. Article 1 (c) defines "service provider" to mean: (i) any public or private entity that provides to users 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 communications service or users of such service. The scope of the Convention's definition is broader than traditional telecommunication or internet service providers, and may extend to a wider class including "application service providers" that offer various services beyond basic telecommunications or internet access. For example, a plain reading of Article 1(c)(ii) suggests that proxy and VPN (virtual private network) services, cloud storage services, certain types of data processing services, some services associated with "big data analytics", large scale directory services and so forth could be included if in some manner linked to Article 1(c)(i) – that is, service providers which offer computing, processing or computational power for any number of applications associated with computer facilitated communications services. Given the broad scope of the definition of "service provider" in the Convention, pronouncements made by Parties to the Convention with respect to whether a service provider is "offering its services in the territory of the Party" may not be restricted to such well-known multinationals such as Facebook or Google. A wide range of entities could be within the purview of Article 18 and as such, a comprehensive answer requires further analysis. Accordingly, Canada is taking a cautious approach in an environment which is evolving, both legally and technologically, and will continue to study this issue.
Croatia	Expressly or implicitly offers a remote access to his services to persons situated in Croatia (direct statement, on-line registration of users with Croatian addresses, communication via .hr domain etc.)regardless of the location of a service provider or

	server. Fails to take reasonable measures to prevent persons situated within Croatian territory to use his services (blocking Croatian IP addresses, refusing to register Croatian users etc.) However, it would not be considered as offering a service in Croatia if user circumvents such measures by hiding true location. Please note that a mere statement that customers are solely responsible for using services within the intended territory, that user undertakes only to use the services in the country in which the services are intended to be used, or similar, by itself would not be considered as a reasonable measure to prevent persons situated within Croatian territory to use his services.
Czech Republic	In general there are 2 possibilities of identifying the service provider offering service on the Czech territory. 1) a service provider is registered according to the Act on Electronic Communication in the Czech Telecommunication office 2) a service provider is not doing business subject to the Act on Electronic Communication and does not have to be therefore registered. In this case service provider is identified as offering a service on the Czech territory according to its real activities and situation is evaluated individually.
Finland	The government proposal preceding ratifying the Convention does not deal with this issue. Because of this there is no clear answer. However it´s possible interpret paragraph 1.b. so that it covers both domestic and foreign providers, including their national representatives, providing services for natural and legal persons locating in the territory.
France	Les forces de Police et de Gendarmerie françaises considèrent que tout fournisseur de service Internet (FSI) accessible depuis un appareil électronique présent sur le sol national est considéré comme offrant une prestation sur notre territoire.
Germany	The obligations of any persons or companies offering telecommunications facilities are statutorily regulated in the "Telecommunications Act" (TKG) of 22 June 2004 and in addition to this in the "Ordinance concerning the Technical and Organisational Implementation of Measures for the Interception of Telecommunications (Telecommunications Interception Ordinance - TKÜV)" of 3 November 2005. The Telecommunications Act contains regulations for subscriber information and traffic data while the Telecommunications Interception Ordinance focuses more on content data. According to section 3 number 6 of the Telecommunications Act a service provider in the definition for the purposes of the Telecommunication Act means a person who, on a wholly or partly commercial basis, either provides a telecommunications service (lit. a), or contributes to the provision of such service (lit. b). For the purposes of the Telecommunications Interception Ordinance, operator of a telecommunications facility shall mean the company that exercises actual control over the functions of a telecommunications facility (section 2 number 4 of the Ordinance). According to these definitions, a service provider can be considered offering a service on German territory if a person or company in the territorial validity of German jurisdiction provides a telecommunications service or contributes to the provision of such service or exercises actual control over the functions of a telecommunications facility.

Hungary	The short answer is, if the service provider is represented in Hungary form corporate law point of view. Our National Media and Infocommunications Authority operate a public register on subscribable public communications services together with the main data of their providers. http://webext.nmhh.hu/hir_szolg/app/index.jsp?lang=1 However, based on the Section 71 of the Hungarian Criminal Procedure Code it is possible to get information from any type of legal entities in order to support criminal investigations.
Italy	The Italian electronic communication rules (Legislative Decree of 1st August 2003 n. 259, with EC origin in the Directives 2002/19, 2002/20, 2002/21, 2002/22 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7th March 2002) do not provide any clarifications about this topic. According to this situation, we can have a) service providers registered according to the electronic communication rules in the Italian Telecommunication Office (Ministero dello Sviluppo Economico) b) service providers which are not doing business subject to the Italian electronic communication rules even if they are offering a service to Italian consumers according to their concrete activities.
Japan	Since it needs to be determined by considering individual circumstances of each service provider, there exists no general answer. Yet, it can be said that service provider is offering a service on Japan's territory when it holds a base such as business offices within Japan's territory. Also, in a case when service providers do not hold a base within Japan's territory, if they offer a service to many and unspecified domestic users on a regular basis, it is possible to say that they are offering a service on Japan's territory.
Latvia	"Cloud" service provider only provides its services within the territory of the Republic of Latvia (not within a Latvian section of the global network) when mentioned service provider is appropriately registered in the Republic of Latvia. Production order may be given directly to the service provider only if a service provider is registered within the territory of Latvia and in strict abidance to Latvian legislation. Rights and responsibilities of a service provider are listed in Electronic Communications Law of the Republic of Latvia (document may be found in attachment to this letter). Electronic Communications Law also regulates volume and procedure of information exchange between service provider and law enforcement organizations in the Republic of Latvia. Requests to foreign law enforcing organizations are being sent with the help of rogatory letter and in accordance to legislation of the republic of Latvia. Within Latvian territory, information is being received on the basis of Cabinet Regulation Nr.820 "Procedures by which Pre-trial Investigative Institutions, Bodies Performing Investigatory Operations, State Security Institutions, Office of the Prosecutor and Court Request and a Merchant of Electronic Communications Transfers Data to be Retained, and Procedures by which Statistical Information regarding Requests of Data to be Retained and Issuing thereof is Compiled" (document may be found in attachment to this letter).
Lithuania	Lithuanian legislation does not explicitly define the notion of "service provider". Nor does it specify the concept of "offering a service on the territory". However in practice and based on the provisions of relevant national laws and implementing acts, we consider that service provider is offering its service on the territory of Lithuania if the provider or its legal representative (records keeper) is

	registered and exercises its economic activity (provision of public communications services or networks) on the territory of Lithuania, irrespective of who are the end-users of the service. So generally speaking, if we have a Lithuanian entity which provides Internet or hosting services to the end-users both in and outside of Lithuania, or which is a legal representative (records keeper) of the provider operating outside of Lithuania, we would consider it to offer a service on our territory, and would therefore be empowered to impose means of criminal procedure on them.
Luxembourg	Dès qu'un résident luxembourgeois, personne physique ou morale, a la possibilité d'avoir recours, sur le territoire luxembourgeois, à un service presté par un fournisseur de services, ce dernier offre une prestation de service sur notre territoire.
Mauritius	Upon being issued with a licence under section 24 of the Information Communication and Technologies Act (Act), the service provider is considered to be offering service. Section 24 (1) of the Act provides: 24. Licensing (1) No person shall operate an information and communication network or service including telecommunication network or service unless he holds a licence from the Authority. The definition of Authority" or "ICT Authority" means the Information and Communication Technologies Authority established under section 4 of the said Act
Moldova	The service provider is offering a service on the territory of the Republic of Moldova at the request of the competent authority, meaning the General Prosecutor's Office of Moldova, during the criminal investigation.
Monaco	L'article 4 de la loi n° 1.383 du 2 août 2011 sur l'économie numérique prévoit que « sont soumises à la présente loi les activités définies au premier alinéa de l'article 2 si la personne qui l'exerce est établie sur le territoire monégasque ou si la personne à qui sont destinés les biens et les services est établie que le territoire de la Principauté."
Montenegro	From the day of registration in the Central Register of the Commercial Court and after decision of the Agency for Electronic Communication and other responsible bodies in the process of establishing of the service provider.
Netherlands	In general criminal investigations and prosecution procedures are regulated in the Dutch Code of Criminal Procedure (Wetboek van Strafvordering, DCCP). In January 2006 the Data Production Orders Act (Wet bevoegdheden vorderen gegevens) enacted several powers to order the production of data. The powers were placed in the DCCP. The powers make a distinction of identifying data, other data and sensitive data. The orders can be given to persons who process the data in a professional capacity; an order for "other" stored data and sensitive data can, however, also be directed at persons who process data for personal use. In order to obtain user data art. 126na DCCP provides for an investigating officer the possibility to order a communications service provider, in case of a crime, to produce user data. User data are name, address, telecommunications number, and type of service. Art. 126n DCCP, concerning traffic data (infra), also comprises the collection of user data. Other information pertaining to the identity of a person may be ordered under art. 126nc DCCP. Art. 126la DCCP defines the term "supplier of communication services" (aanbieder

	van een communicatiedienst) as the natural or legal person who in the execution of a profession or business offers to users of his services the possibilities to communicate by means of a computer system, or processes or stores data for such services or for the user of the services. This definition encompasses the Telecommunication providers (now often mixed services), which are providers offering public telecommunication networks and services and who are regulated also in the Dutch Telecommunications Act. Companies like Google, Facebook / Instagram, Skype, Microsoft, Apple fall under the definition of article 126la.
Panama	With regard to domestic production orders for subscriber information, every provider is requested to provide the information that is relevant to the investigation. Among the items of information about subscribers that providers are requested to provide are : all the subscriber's particulars, domicile or geographic address, telephone, invoicing and payment data. Panama has Law 51 of 2009, that regulates the technological storage of data (preservation of electronic documents and document files, including the legal validity of technological storage, judicial value of technologically-stored documents, minimum guarantees which must be fulfilled by the technological storage system, statement of practices regarding the technological storage of documents, authentication of technologically-stored documents, recognition of documents technogically stored abroad).
Philippines	A service provider is offering a service in the Philippine territory if: (1) it provides to users of its service the ability to communicate by means of a computer system; or (2) it processes or stores computer data on behalf of such communication service or users of such service. [Section 3 (n), Republic Act No. 10175 or the "Cybercrime Prevention Act of 2012" ("CPA"); Section 3 (ff), Rules and Regulations Implementing Republic Act No. 10175, otherwise known as "the Cybercrime Prevention Act of 2012" ("CPA-IRR")]
Portugal	A provider is offering a service when its services are specifically directed to those who live on that territory - meaning, when the provider seeks customers on that territory and develops the type or profile of the service in view of costumers on that territory. The service can be particularly directed to costumers on that territory or even generically directed to all the costumers in the world, including the costumers living on a given territory. As example, when Google creates and offers its search engine under the domain google.pt it can be considered that is offering the services to Portuguese costumers.
Romania	When the service provider is represented in Romania, namely the servers delivering the service are situated in our country i.e. legal entity established under Romanian legislation or legal representation recognized by Romanian legislation.
Slovakia	Article 5 para. 1 of the Act No. 351/2011 Coll. on electronic communications as amended stipulates that a service provider is any person that provides the network or service; providing of network or service in the area of electronic communications for a third party is considered for business. Further details are regulated by the said Act.
Slovenia	In Article 3 (Definitions) of Law on Electronic Commerce, the service provider is any private or legal person who provides information society services, which are normally provided for remuneration, at a distance , by electronic means and at the individual

	request of a recipient of services.
Spain	According to Art. 2 of Act 34/2002 on Information Society Services and Electronic Commerce (LSSICE), a service provider is understood to be established in Spain when its registered office is located in Spanish territory and also when – even if domiciled in another State – its services are provided through a permanent establishment located in Spain. Article 3, in turn, makes the same legal system applicable to service providers settled in another European Union (EU) or European Economic Area (EEA) Member State when the recipient of the services is based in Spain and the services concern certain matters. According to Article 4 of LSSICE, service providers addressing their services specifically towards Spanish territory, although established in third countries, shall be subject to the Spanish regulations provided this does not contravene the provisions of applicable international treaties or conventions.
Switzerland	Entities registered in our country are regularly considered to offer their services (if they do so) on our territory. On the other hand, it may not be sufficient that services such as content of websites can simply be made available and read via a computer on our territory. It may be necessary that a natural or legal person located on the territory contributes in some way to the offering of services. According to the understanding of our national courts, article 18 para. 1 b of the Convention does not constitute a directly applicable basis for a trans-border request to store or provide data.
Tonga	When the service provider is based in Tonga and providing its services to the citizens of Tonga.
United Kingdom	If the data is stored in the UK. If the service provider holds itself out as being based within the jurisdiction, they are regarded as offering a service in the territory.
United States	We do not have fixed criteria. We assess the totality of the circumstances.

b. Thus, when do you consider that you can deliver a domestic production order for subscriber information directly to the service provider offering the service?

Australia	Section 178 of the TIA Act allows an authorised officer of an enforcement agency to authorise a service provider to disclose historic telecommunications data if the disclosure is reasonably necessary for the enforcement of the criminal law. Historic telecommunications data is data that is already in existence when the authorisation is made. Section 178A of the TIA Act allows an authorised officer of a police force to authorise a service provider to disclose historic telecommunications data to assist in locating a missing person. Section 179 of the TIA Act allows an enforcement agency to authorise a service provider to disclose historic telecommunications data if the disclosure is reasonably necessary for the enforcement of law imposing a pecuniary penalty or for the protection of the public revenue. Section 180 of the TIA Act allows a criminal law-enforcement agency to authorise a service provider to disclose prospective telecommunications data for up to 45 days if

	the disclosure is reasonably necessary for the enforcement of an offence punishable by imprisonment for three years or more. Prospective data is telecommunications data collected in real-time, or close to real-time.
Bosnia and Herzegovina	**Brcko District of Bosnia and Herzegovina - The District Police - Crime Investigations Police** A domestic production order for a subscriber information can be sent directly to the service provider in case of founded suspicion of acommitted crime within our responsibility of investigation. **Regulatory Agency for communication** Service providers shall not directly respond to the request made by the judicial or other bodies from abroad. The Party should have an opportunity, after having received a request, to perform a control procedure to see if there is the respect of the standards referring to the protection of personal data, democratic principles, specific political, economic and security interest of the Party **Federal Ministry of Internal Affairs - Federal Police Administration** In accordance with the positive legislation, the police agencies shall not directly address the service provider for the delivery of data, but they shall be obtained via the competent court.
Bulgaria	Domestic production order can be delivered according to the provisions in the Electronic Communications Act – art. 251b and art. 251c only with regard to investigation of a serious crime (punishable by five years or more) or with regards to national security. The domestic production order has to be a court order. The law only regulates the orders to providers which are registered with the Commission on Electronic Communication. There are no regulations on orders to foreign service providers. Electronic Communications Act Art. 251b. (New - SG. 24 of 2015, effective 03.31.2015) (1) The enterprises providing public electronic communications networks and / or services store for 6 months data generated or processed in the process of their activities, which are necessary for: 1. trace and identify the source of the connection; 2. identification of the destination of the connection; 3. identify the date, time and duration of the connection; 4. identification of the type of connection; 5. identification of electronic communication device of the user or what presents to his terminal; 6. establishment of an identifier of the used cells. (2) The data under para. 1 shall be kept for the needs of national security and the prevention, detection and investigation of serious crime. (3) Other data, including revealing the content of the messages can not be stored in this way. (4) The data under para. 1 is processed and stored in accordance with the requirements of the protection of personal data. Art. 251c. (New - SG. 24 of 2015, effective 03.31.2015) (1) Right to want to consult the data under Art. 251b para. 1 where data are necessary for the performance of

	their duties are: 1. Specialized directorates, regional directorates and autonomous territorial departments of the State Agency "National Security"; 2. General Directorate "National Police" General Directorate "Combating Organized Crime" and its territorial units, General Directorate "Border Police" and its territorial units, "Internal Security", the Sofia Directorate of the Interior and the regional directorates of the Ministry of interior; 3. "Military Information" and "Military Police" of the Ministry of Defence; 4. (amend. - SG. 79 of 2015, effective 01.11.2015) The State Agency "Intelligence". (2) Access to the data of art. 251b para. 1 is given after a reasoned written request from the head of the bodies under para. 1 or authorized person, including: 1. The legal basis and purpose for which access is required; 2. The registration number of the file for which the need for a access is required, and user data, when known; 3. The data which should be reflected in the report; 4. The period of time for the report; 5. Complete and comprehensible indication of the facts and circumstances justifying the purpose of art. 251b para. 2; 6. The designated official to whom to provide the data. (3) For the requests the bodies under par. 1 shall keep a special register which should not be public.
Canada	Canada's new production order regime in the Criminal Code was updated with the Protecting Canadians from Online Crime Act which came into force on March 10, 2015. Production orders are not constrained by a particular type of person (natural or artificial) and as such a production order can be directly served on any person, including any type of service provider, if that service provider is on our territory. The data in question must be in that person's possession or control (actual or constructive). In a number of respects this is similar to the European Union's concept that the location of the data controller is relevant but not the location of the data as such (the data could be stored outside Canada's territory). Authority to issue production orders is constrained by the territorial limits of the Criminal Code of Canada. Consistent with international law concepts of sovereignty and jurisdiction, Canadian courts can issue production orders in respect of service providers on Canadian territory and their compliance is then enforceable by Canadian courts. Given that Parliament has the power to authorize extra-territorial action but must do so expressly, direct serving of production orders beyond Canadian territory would likely require new legislative provisions.
Croatia	The service provider should have at least subsidiary with Croatian address in order to deliver a domestic production order for subscriber information directly. Otherwise, an international legal assistance would have to be used.
Czech Republic	If the law enforcement authority qualifies that service provider is offering service on the Czech territory, domestic production order is delivered immediately.
Finland	A production order is possible to deliver in the margins mentioned above. Also the last part of paragraph 1.b concerning the possession or control of information has to be taken into account. This means that the location of the data is meaningful in consideration.
France	Dès lors que des besoins opérationnels sont constatés et que des fournisseurs de service accessibles en France sont susceptibles d'apporter leur aide et assistance, les autorités françaises considèrent qu'elles peuvent les requérir directement, sous

	contrôle de l'autorité judiciaire. Toutefois, seuls les FSI de droit français sont susceptibles d'être requis directement en raison de l'opposabilité du droit français. Concernant les FSI de droit étranger, le droit français ne leur étant pas opposable, les demandes de données ne peuvent être coercitives. Ainsi, des conventions partenariales ont été mises en place par le Ministère de l'Intérieur avec de nombreux opérateurs étrangers afin que ceux-ci puissent être sollicités directement sans pouvoir pour autant y être contraints. Outre le fait de garantir une réponse aux demandes formulées par les enquêteurs, ces conventions normalisent les procédures de demandes de données en trois catégories : - N1 : affaires générales - N2 : Atteintes graves aux personnes et aux biens - N3 : La lutte contre le terrorisme et les atteintes aux intérêts fondamentaux de la nation Les FSI signataires de ces conventions s'engagent à fournir les données techniques/déclaratives permettant d'identifier un utilisateur français; les demandes de contenus ne sont possibles que par demande de coopération judiciaire internationale.
Germany	The answer on this question depends on whether the seat of the provider is located on German territory or abroad. In the latter case German authorities would have to turn to the authorities of the state hosting the provider to request the execution of the production order based on the applicable MLA instruments. In the first case (seat of the provider on German territory) the following rules apply: Pursuant to section 111 [Data for Information Requests from Security Authorities] subsection (1) of the Telecommunications Act any person commercially providing or assisting in providing telecommunications services and in so doing allocating telephone numbers or providing telecommunications connections for telephone numbers allocated by other parties is to collect, prior to activation, and store without undue delay subscriber information. The subscriber information contains the telephone numbers or any other identification of allocation, the name and address of the allocation holder, the date of birth in the case of natural persons, in the case of fixed lines, additionally the address for the line, in case of surrendering a mobile terminal equipment beside a mobile allocation, the device number of this equipment, and the effective date of the contract. The information must be collected and stored even if such data are not required for operational purposes of the company. Where known, the date of termination of the contract is likewise to be stored. *Directly* to the service provider you can deliver a domestic production order for subscriber information pursuant section 113 of the Telecommunications Act in the Manual Information Procedure. According to section 113 subsection (1) sentence 1, any person commercially providing or assisting in providing telecommunications services is authorized to use data collected under sections 95 and 111 to answer the information requests submitted by the competent bodies in accordance with the further requirements of section 113. The information is to provide by the service provider to the extent required for the prosecution of criminal or administrative offences or for averting danger to public safety or order and for the discharge of the legal functions of the federal and state authorities for the protection of the Constitution, the Federal Intelligence Service and the Federal Armed Forces Counter-Intelligence Office, if the requests are submitted by the competent body in textual form and the regulation that allows the collecting of data is named. The competent bodies bear the responsibility for the legitimacy of the request.

	E.g., for the purposes of criminal procedure, the regulation that permits the request for information is regulated in section 100j of the German Criminal Code. Collecting data is insofar allowed as necessary to establish the facts or determine the whereabouts of an accused person. Not *directly* to the service provider, but to the Regulatory Authority (so called "Bundesnetzagentur") a domestic production order for subscriber information can be delivered in the Automated Information Procedure according to section 112 of the Telecommunications Act. Therefore any person providing publicly available telecommunications services shall store, without undue delay, data collected under section 111 in customer data files. Information from the customer data files according to section 112 subsection (1) shall be provided to competent bodies such as the courts and criminal prosecution authorities (1), the federal and state police enforcement authorities for purposes of averting danger (2), the Customs Criminological Office and customs investigation offices for criminal proceedings and the Customs Criminological Office for the preparation and execution of measures under section 23a of the Foreign Trade and Payments Act (3), the federal and state authorities for the protection of the Constitution, the Federal Armed Forces Counter-Intelligence Office and the Federal Intelligence Service (4), the emergency service centres according to section 108 and the service centre for the maritime mobile emergency number "124124" (5), the Federal Financial Supervisory Authority (6) and the authorities responsible under state legislation for the prosecution of administrative offences as provided for by section 2(1) of the Undeclared Work Act, via central inquiry offices (7). The information shall be provided at all times, as far as such information is needed to discharge their legal functions and the requests are submitted to the Regulatory Authority by means of automated procedures.
Hungary	In principle, if the concerned service provider is offering a service in Hungarian territory and the concerned data is here, service provider should answer and give the data. If it is not the case, service provider should refuse the request. There is no specific rule or procedure on data from cloud, thus law enforcement and judicial authorities following an approach that treats all data at the same way. This means from practical point of view that, since LEAs and Prosecutors should not be aware the concrete location of the concerned data, they can issue an order and if the service provider offering service in Hungarian territory gives the data based on the request of LEAs and prosecutors they can presume that data was here. As far as there is no concrete information on original location of the provided data in the answer its source cannot be checked from jurisdiction side.
Italy	A Public Prosecutor's production order can be delivered to an ISP whether or not he has based on the Italian territory. The legal problem is that the Italian criminal procedural code doesn't have any instruments to enforce orders abroad, beyond the ordinary international MLA channels.
Japan	Respecting the sovereignty of other state, domestic production order for subscriber information is, in principle, delivered directly to the service provider that is located within Japanese territory.
Latvia	"Cloud" service provider only provides its services within the territory of the Republic of Latvia (not within a Latvian section of the global network) when mentioned service provider is appropriately registered in the Republic of Latvia. Production order may be given directly to the service provider only if a service provider is registered within the territory of Latvia and in strict abidance to Latvian legislation. Rights and responsibilities of a service provider are listed in Electronic Communications Law of the Republic of Latvia (document may be found in attachment to this letter).

	Electronic Communications Law also regulates volume and procedure of information exchange between service provider and law enforcement organizations in the Republic of Latvia. Requests to foreign law enforcing organizations are being sent with the help of rogatory letter and in accordance to legislation of the republic of Latvia. Within Latvian territory, information is being received on the basis of Cabinet Regulation Nr.820 "Procedures by which Pre-trial Investigative Institutions, Bodies Performing Investigatory Operations, State Security Institutions, Office of the Prosecutor and Court Request and a Merchant of Electronic Communications Transfers Data to be Retained, and Procedures by which Statistical Information regarding Requests of Data to be Retained and Issuing thereof is Compiled" (document may be found in attachment to this letter). See attached laws
Lithuania	Production order in the sense of Art 18 Para 1.b. of the BC corresponds to a national procedural coercive measure set out in Art 155 of Criminal Procedure Code of the Republic of Lithuania – "Public Prosecutor's Right to Get Acquainted with the Information". Pursuant to this provision, public prosecutor has the right to come to any state or municipal, public or private entity, company or organisation, and demand to be given access to relevant documents or other data, allowed to make records or copies of documents and data, and to obtain relevant information in writing, if the documents or data are needed for the purposes of an ongoing investigation. To exercise this right, public prosecutor shall issue a resolution and get it approved by a pre-trial investigation judge. Public prosecutor also may delegate the exercise of this right to a pre-trial investigator, conducting the investigation. Use of this right may be restricted by law. However, current Lithuanian legislation does not contain any restrictions with regard to whether service provider offers its service on the Lithuanian territory or not. In practice this means that if data that is supposed to be in the possession or control of a service provider is needed for the purposes of an ongoing investigation, public prosecutor is allowed to deliver the resolution (domestic production order) envisaged by Art 155 of the CPC to the service provider irrespective of whether it offers its service on the territory or outside of Lithuania. So, domestic production order can be delivered not only to Lithuanian service providers, but also to a foreign service provider directly and the data obtained can be used in an ongoing investigation, provided that the addressed service provider agrees to disclose the requested data. Also, please note that pursuant to Art 20 of the CPC only court has the right to decide whether the data and other evidential information collected by the prosecution are admissible as evidence.
Luxembourg	Dès qu'un résident luxembourgeois, personne physique ou morale, a eu recours, sur le territoire luxembourgeois, à un service presté par un fournisseur de services
Mauritius	The service provider cannot be delivered with a domestic production order directly. A Judge in Chambers order needs to be sought and the Applicant making the application for the order must satisfy the Judge that such an order is warranted.

Moldova	Our authorities deliver a domestic production order when the prosecutor sends the ordinance to service provider or when some criminal investigation acts need a court authorization.
Monaco	Une injonction de produire directe peut être donnée à tout fournisseur établi à Monaco ou fournissant des biens ou des prestations à des personnes résidant à Monaco
Montenegro	Only based on the Court order or based on the request of the Prosecution Office. In urgent cases directly from the service provider but later it has to be justified by Court order.
Netherlands	In principle Dutch law allows for serving production orders to all supplier of communication services defined in article 126la DCCP. The article 126ng section 1 provides this power for subscriber and traffic data. However such production orders cannot be enforced when they are served to companies in foreign jurisdictions. In those cases either mutual legal assistance is sought or companies are contacted directly.
Panama	As we stated in our previous answer, Panama has law which regulate requests by a subscriber for information from service providers. As set forth in the Code of Criminal Procedure, each time a request for information is received by a service provider it must be accompanied by an order from a competent authority. If no such order exists, service providers must not provide information, even if an informal request is made for information concerning a subscriber.
Philippines	Law enforcement authorities, such as the Philippine Department of Justice Office of Cybercrime (DOJ-OOC), National Bureau of Investigation-Cybercrime Division (NBI-CCD), and Philippine National Police - Anti-Cybercrime Group (PNP-ACG), upon securing a court warrant, can issue an order requiring any person or service provider to disclose or submit subscriber's information, traffic data or relevant data in his/its possession or control within seventy-two (72) hours from receipt of the order in relation to a valid complaint officially docketed and assigned for investigation and the disclosure is necessary and relevant for the purpose of investigation. (Section 14, CPA; Section 14 CPA-IRR) The process envisioned under Section 14 of CPA/CPA-IRR is likened to a subpoena, which can be issued by executive agencies as an adjunct of their investigatory powers. The disclosure order is an enforcement of a duly issued court warrant, and thus requires judicial intervention. (Disini vs. Secretary of Justice; G.R. No. 203335; 11 February 2014) As an exception to the requirement of court intervention, An ISP shall, upon the request of proper authorities, furnish the particulars of users who gained or attempted to gain access to an internet address which contains any form of child pornography. (Section 9, Republic Act No. 9775 or the "Anti-Child Pornography Act of 2009")
Portugal	The order can be delivered to service providers whether or not they are based/have an office on the Portuguese territory. According to the Portuguese law it is not forbidden to ask information to someone outside the territory. Thus, to request information via a production order is valid and will be valid the evidence eventually provided. However, if it is necessary to enforce the order, if it is not voluntary replied, is an issue. The Portuguese law does not provide any tool or instrument to enforce orders abroad, beyond the classic international mutual legal assistance channels.

Romania	When the service provider is represented in Romania.
Slovakia	It should be noted that the current situation is the consequence of the Court of Justice of the European Union´s decision of 8 April 2014 (Joined cases C-293/12 and C-594/12) that Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC is invalid. On 29 April 2015 the Constitutional Court of the Slovak Republic decided that some of the provisions of the Act No. 351/2011 Coll. on electronic communications as amended, as well as one provision of the Act No. 301/2005 Coll. Code of Criminal Procedure as amended and the Act No. 171/1993 Coll. on Police Corps as amended were contrary to the Constitution of the Slovak Republic, the Bill of Fundamental Rights and Freedoms (Constitutional Act No. 23/1991 Coll.), the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union. In particular, the decision was related to Article 116 of the Code of Criminal Proceedings, which used to be applied for the purposes of obtaining subscriber information, traffic and content data from service providers. Meanwhile, the new legislation has been drafted. If it is adopted by the Slovak parliament, all three categories of data will be subject to strict legal conditions similar to interception of telecommunication.
Slovenia	We consider that we can deliver domestic production order if service provider effectively pursues an economic activity for an indefinite period in an area where it is situated (for example Microsoft Slovenia).
Spain	When, in the exercise of their functions, the Public Prosecutor or Judicial Police need to know the ownership of a phone number or of any other communication means or, in the opposite sense, require the telephone number or the identifying data of any communication means, can turn directly to the providers of telecommunication services, of access to a telecommunications network or of the information society services who will be obliged to meet the requirement, under penalty of incurring the offence of disobedience Such request can be addressed either to the ISP located in Spain or to those based in other countries, as we have aforementioned, the Spanish legal system does not make any difference as regards to that matter.
Switzerland	National prosecution authorities are not supposed to use (domestic) production orders directly vis-à-vis foreign entities, even if they may be considered, in the end and due to a lack of means of enforcement, as tools to activate a voluntary co-operation from the foreign entity. MLA procedures apply. In situation where authorities detect a natural or legal person contributing to the offering of services located on the territory, a domestic production order may be used (depending, of course, also on the probability of successfully collecting the data sought after).
Tonga	Section 11(b) of the Computer Crimes Act 2003 provides that a production of data order can be issued to "an internet service provider to produce information about persons who subscribe to otherwise use the service. This can be done for the purposes of a criminal investigation or criminal proceedings.
Turkey	When the courts need more information in order to progress a specific investigation, law enforcement has to get in touch with the service provider and demand what is

	asked by claiming an appropriate court order.
United Kingdom	Some CSPs disclose non-content (basic subscriber information (BSI) or traffic) when UK domestic process is served (section 22(4) RIPA Notice) on the basis U.S. Law Enforcement have a reciprocal power. This is referred to as "voluntary disclosure" by the CSPs as they provide on a goodwill basis and without any statutory basis. However CSP policies can be inconsistent leading to confusion about the best way to secure evidence.
United States	See above.

c. In your experience, what are the criteria, conditions or circumstances that make service providers accept or decline such a request?

Australia	Subsections 313(1) and (2) of the *Telecommunications Act 1997* require service providers to do their best to prevent their networks and facilities from being used in, or in relation to, the commission of criminal offences. In addition, section 313(3) establishes an obligation for service providers to provide agencies with 'reasonably necessary assistance' in enforcing the criminal law (amongst other purposes). As such, if a service provider receives a valid authorisation pursuant to the above sections in the TIA Act (as outlined in the response to **b.**) then the service provider must meet the request. The Australian Federal Police (AFP) note that in their experience the only reason for declining a request (besides legislative compliance) would be instances when the service provider no longer has the information.
Bosnia and Herzegovina	**Brcko District of Bosnia and Herzegovina - The District Police - Crime Investigations Police** From our experience, service providers act upon direct requests for submission of subscriber information. However, it depends on the type of requesteddata, a service provider'sterritory/country, and aservice providers'policy on the data provision. The Criminal Procedure Code of the Brcko District of Bosnia and Herzegovina stipulates in its Article 72aa dispatchof a court orderto a telecommunications operator or the other legal entity providing the telecommunication servicesfor provision of the information on the use of telecommunication services in cases of grounded suspicion of committed crime, where such data could be used as evidence in criminal proceedings or helpwith the collection of information usefulfor the criminal proceedings. This, however,also means that service providers can refuse to act upon a direct request of the police, especially if requested data concern the use of services (traffic) or the content. **Regulatory Agency for communication** / **Federal Ministry of Internal Affairs - Federal Police Administration** The Internet Service Providers shall act in accordance with the Court orders and the Courts shall evaluate the validity of the request for the delivery of data.
Bulgaria	Service providers, registered with the Electronic Communications Commission are obliged by the law to follow the court order.

Canada	Following the Supreme Court decision in R v. Spencer , service providers (in particular, telecommunications service providers including internet access providers) in Canada will not disclose much if any information pertaining to their subscribers (including subscriber names and addresses) without a production order. However, some service providers take the view that the requested information is not in their possession or control, particularly if these companies are subsidiaries of a foreign (often American) parent corporation: such companies maintain that the parent corporation controls the data, so a production order cannot compel the subsidiary to release what is not under their control. Law enforcement may then resort to mutual legal assistance to obtain the data from the foreign parent company.
Croatia	Persuant to articles 259/1, 261/2,263/1,2 of the Act on Criminal procedure all production orders should have a statement that the person who fails to comply with the order shall be imposed a fine amounting to HRK 50,000.00 by the investigating judge upon the motion with a statement of reasons of the State Attorney, and should this person even after such a fine not comply with the order, he may be sentenced to imprisonment until the order is executed, but no longer than one month. Additional conditions are not regulated by law, with exeption of instructions neccessary to comply with the production order (deadline for delivery of data etc.).
Czech Republic	One of the most important factors is time and data retention. In general police has to state that it is very individual and depends on many circumstances.
Finland	From the constitutional and legislative point of view requests from other states should be sent to competent authorities, which enforce the measure in accordance with national law and international obligations on mutual assistance. As an executing state, Finland is able to act on 24/7 basis. As concerning obtaining of subscriber details, the Police Act, Chapter 4 and Section 3, is applied: The police have the right to obtain from a telecommunications operator and a corporate or association subscriber the contact information about a subscription that is not listed in a public directory or the data specifying a telecommunications subscriber connection, an e-mail address or other telecommunications address, or telecommunications terminal equipment if, in individual cases, the information is needed to carry out police duties. In addition, under the same provision, at the request of a commanding police officer, the police have the right to obtain any information from a private organization or person necessary to prevent or investigate an offence, notwithstanding business, banking or insurance secrecy binding on members, auditors, managing directors, board members or employees of an organization. In Finland, subscriber details are not covered with a high privacy protection. For instance, telephone subscriber details are usually public and available for anyone via service numbers or the Internet, unless the concerned holder has not limited the access to the information.
France	En droit français, le fait de ne pas répondre à une réquisition judiciaire est passible d'une amende pénale (Art 60-1 Code de Procédure Pénale). Dans le cadre d'une urgence vitale, les dispositions de l'article 223-6 du Code Pénal peuvent également être opposées au FSI. Art 223-6 CP : Quiconque pouvant empêcher par son action immédiate, sans risque

	pour lui ou pour les tiers, soit un crime, soit un délit contre l'intégrité corporelle de la personne s'abstient volontairement de le faire est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. Sera puni des mêmes peines quiconque s'abstient volontairement de porter à une personne en péril l'assistance que, sans risque pour lui ou pour les tiers, il pouvait lui prêter soit par son action personnelle, soit en provoquant un secours. Concernant les FSI de droit étranger, l'implantation sur le territoire national de division juridique et/ou commerciale permet de faciliter le traitement des demandes même si celui-ci demeure au bon vouloir des sociétés sollicitées. Dès lors, en raison soit de leur politique interne soit de la législation nationale du siège de leur société, certains FSI étrangers ne répondent pas ou a minima aux sollicitations des autorités françaises. Par exemple, certains fournisseurs de service mettent en avant l'absence d'incrimination locale liée à la demande reçue ou font état leur politique interne de protections des données de leurs clients.
Germany	Under German law, the conditions that make service providers accept or decline a data information request are regulated in sections 111 – 113 of the Telecommunications Act outlined in the answer to the question 1 lit. b (see above).
Hungary	Usually traffic data comes without MLA but content data only if there is an issued or prejudicated MLA request.
Italy	ISPs based abroad (especially Facebook, Google and Microsoft) usually accept requests and provide information if the request is issued according to the Italian law and also respects their law enforcement policies.
Japan	While such responses differ among service providers, there is a case that a service provider offering services on Japan's territory declines a request due to a reason that its business location has no authority to respond to such request. Nonetheless, a part of such corporations accept the request on a part of crime such as murder, sexual assault, and sexual exploitation of children.
Latvia	"Cloud" service provider only provides its services within the territory of the Republic of Latvia (not within a Latvian section of the global network) when mentioned service provider is appropriately registered in the Republic of Latvia. Production order may be given directly to the service provider only if a service provider is registered within the territory of Latvia and in strict abidance to Latvian legislation. Rights and responsibilities of a service provider are listed in Electronic Communications Law of the Republic of Latvia (document may be found in attachment to this letter). Electronic Communications Law also regulates volume and procedure of information exchange between service provider and law enforcement organizations in the Republic of Latvia. Requests to foreign law enforcing organizations are being sent with the help of rogatory letter and in accordance to legislation of the republic of Latvia. Within Latvian territory, information is being received on the basis of Cabinet Regulation Nr.820 "Procedures by which Pre-trial Investigative Institutions, Bodies Performing Investigatory Operations, State Security Institutions, Office of the Prosecutor and Court Request and a Merchant of Electronic Communications Transfers Data to be Retained, and Procedures by which Statistical Information regarding Requests of Data to be Retained and Issuing thereof is Compiled" (document may be found in attachment to this letter). See attached laws

Lithuania	Domestic production order as set out in Art 155 of Criminal Procedure Code of the Republic of Lithuania is legally binding on Lithuanian service providers. In the event of refusal to comply with the lawful request of a court, public prosecutor or pre-trial investigator, a fine imposed on the refusing provider. Whereas with foreign service providers disclosure of data directly to foreign law enforcement authorities is based on a good-will principle, and domestic production order is only one of the criteria proving that the request is legit, approved by necessary national authorities, and that the data requested is actually needed in an ongoing investigation. Nevertheless, domestic production order does not legally commit foreign service providers to anything. Should they consider that the submitted request is not in line with their policy or applicable laws, they may deny the request and suggest to use MLA procedure. In our experience, foreign service providers tend to cooperate with the law enforcement outside their country of residence rather well. Most of them (especially bigger companies, such as Google, Facebook, Microsoft and alike) have established facilitated procedures for direct cooperation and disclosure of their records. Noteworthy to say, though, that direct cooperation is more frequent with the foreign companies that provide social communication services rather than Internet or hosting service providers. In order to have requests based on a domestic production order accepted and the requested data disclosed, there are several points about domestic production orders to keep in mind: - They must be issued or approved by court; - They must be translated into English; - They should preferably be sent from a SPOC; - They should contain clear reference to the entity (account, IP address, other identifier), sufficient information demonstrating the link between the entity and the investigated criminal offence; - Requests in relation to investigations of criminal offences, related to freedom of speech, tend to be denied, especially by U.S.-based service providers. For this type of criminal offences, MLA procedure is to be used. - Only basic subscriber information and traffic data (access logs) may be obtained on the basis of a domestic production order. For content data, MLA procedure is to be used.
Luxembourg	Il faut qu'il puisse vérifier de manière effective que le recours à son service ait eu lieu sur le territoire luxembourgeois et par un résident luxembourgeois.
Mauritius	Once there is an order of the Court, the service provider needs to comply with same. However, since there is no law which provides for data retention by service provider, it could be the case that the service providers are unable to comply with the Judge's order as the data is no longer available and depending on their policies as to the length of time for data to be retained.
Moldova	The service providers cannot refuse any of the prosecutor's requests and pursuant to art. 7 of the Law no. 20 on prevention and combating Cybercrime, the service providers have the following obligations: a) to keep records of service users; b) provide the competent authorities traffic data information, including data about

	illegal access to information from the computer system, about attempts to introduce illegal content, about the violation by responsible persons of the rules for collecting, processing, storage, dissemination, sharing information or rules of protection of information system provided due to information status or its degree of protection if they contributed to the acquisition, distorting or destroying information or caused other serious consequences, disrupting the functioning of systems, other computer crimes; c) to execute, in conditions of confidentiality, the competent authority request on the preservation of the computer data or data concerning traffic information, to which there is a danger of destruction or alteration, etc.; d) to submit to the competent authorities, pursuant to a request made under the law, user data, including the type of communication and service used by the user, the method of service payment; e) to take security measures by using certain procedures, devices or specialized computer programs which help with access to a computer system to be restricted or prohibited to unauthorized users; f) to ensure monitoring, supervision and retention of traffic data to identify the service providers, service users and the channel through which the communication was sent; g) to ensure the deciphering of information contained in data packets of network protocols preserving these data, etc. (2) Where traffic data information is in the possession of several service providers, the requested service provider is obliged to immediately send to the competent authority the information necessary to identify other service providers.
Monaco	L'unique fournisseur de services numériques en Principauté, MONACO TELCOM, défère systématiquement aux requêtes qui lui sont adressées par les services de la Direction de la Sureté Publique monégasque.
Montenegro	In the case of Court order the request cannot be declined. Request of Prosecution Office can be declined based on the Personal Data Protection Law or due to late submission of the request (retention obligation of 6 months).
Netherlands	Various "foreign" internet service providers, among which are the big US corporations, tend to be responsive to requests of Dutch law enforcement and the judiciary. In may cases these requests take the "administrative" form of a production order, which means that the Dutch regulations on when, what and who remain intact. Common conditions that make that foreign service providers accept the request are: - The requests must come from a single point of contact (SPOC). - They are restricted to non content data; subscriber and traffic data (US law = "subscriber information", "transactional information") - The requests have to be processed as if they were to be served nationally and then handed in to the SPOC. - The LEA SPOC communicates with the providers SPOC and they use "agreed formats". - For content data a MLA request is mandatory. One issue "under debate" is whether the foreign provider will inform the customer on the request made. A standard clause in the Dutch requests is that the ISP will not

	disclose the request to the customer. But some providers have publicly announced that they will change their policies in a way where they will disclose in an early stage.
Panama	If an authority requests information in an investigative process, providers have a duty provide information requiring them. And they cannot be rejected, this is mandated by law and its breach involves the application of sanctions.
Philippines	Based on Philippine experience, service providers respond to requests but their response is that they are unable to comply due to the absence of a court order. At times, service providers claim or assert their subscribers' right to privacy. Furthermore, service providers decline a request alleging that the data/information being requested is unavailable.
Portugal	For some years, Portugal developed the practise of requiring information to a number of service providers based in the United States. The context of this process is explained bellow, in the reply to question 2.a. This experience shows that the providers accept requests and provide information if the request is issued according to the Portuguese law and also respects the American regulations.
Romania	The Romanian legislation is not applicable to a foreign legal person. Thus production orders can be sent abroad only through rogatory letters. The Criminal Procedure Code of Romania is applicable only on the territory of Romania.
Slovakia	Please, see a respond to question b). If draft legislation is approved by the Slovak parliament, there would be a legal obligation for service providers to provide data on the basis of a court order.
Slovenia	Conditions are: they must have probable cause for criminal act, request must come from criminal justice authority (police, public prosecutor, judge), sometimes they decline because they don't have no longer records of subscribers.
Spain	So far and based in our experience, the large US companies usually address –without processing International Letters Rogatory- the requests for direct information from Spain on data relating to subscribers made –in any case- through judicial order as provided for in our domestic law. As mentioned above, after the entry into force of the procedural reform and more specifically of the new article aforementioned (588 ter m), the judicial authorization to obtain subscribers information is not required in Spain but the request can be directly made either by the Public Prosecutor or the Judicial Police. We are eager to see which criterion shall be followed by these companies when requests are to be made in that manner, that is to say, without judicial authorization since at present, we lack experience in relation to this matter.
Switzerland	Service Providers operating on the territory do regularly have a basic interest to comply with requests or orders from prosecution authorities. In situations where the factual or legal circumstances are unclear, dialogue between the requesting authority and the ISP are necessary and often successful.
Tonga	In Tonga, the service providers are normally compliant with orders that are issued by the Courts. However there are times where service providers cannot comply with the request as the information are stored out of Tonga.
Turkey	The data preservation periods for the service providers are stated in Law 5651. If the competent authorities request the information from any service provider they are supposed to provide the data for the court, if available.

United Kingdom	A RIPA Notice pursuant to section 22(4) is the UK domestic equivalent to a U.S. administrative subpoena for basic subscriber information. It also is dependent on the supplier; some providers require a touchpoint in the EU (e.g. Google) and Apple will only provide information on their prescribed form. If an authorised request is made, it will be complied with (provided they still hold the information – they must hold call data for a year, and other details longer).
United States	Sometimes, storage of data outside the US or the absence of employees on US territory.

Q 2. Direct cooperation between criminal justice authorities (such as police, prosecutors or courts) and foreign service providers

Transparency reports published by many service providers indicate that service providers often respond to request for data that they receive directly from criminal justice authorities. Thus:

a. What are your policies, practices and experiences regarding direct requests (a) subscriber, (b) traffic, and (c) content data to a foreign police agency, prosecution service or court?

Australia	*Requests by Australian agencies to foreign police agencies, prosecution services or courts* Requests by Australia to foreign countries for the content of communications and for subscriber and traffic data that is to be used in evidence are governed by the *Mutual Assistance in Criminal Matters Act 1987*. Mutual assistance requests are made by the Attorney-General and Minister for Justice on behalf of: - a law enforcement agency - a prosecuting agency - a defendant in a criminal matter (in some cases). Australia can make requests to any country and receive requests from any country. Requests by Australian police agencies to foreign police agencies for subscriber and traffic data for non-evidentiary purposes can, in some cases, be made on a police-to-police basis, in accordance with arrangements with the relevant foreign police agency, and depending on the relevant laws of the foreign country. *Requests to Australian police agencies by foreign police agencies, prosecution services or courts* Requests to Australia by foreign countries for the content of communications and for the collection (and subsequent disclosure) of traffic data in real-time, are governed by the *Mutual Assistance in Criminal Matters Act 1987*. Mutual assistance requests by foreign countries are considered by the Attorney-General and Minister for Justice. Access to prospective telecommunications data is only permitted for the purpose of investigating a foreign offence carrying a penalty of imprisonment for at least three years and, again, the Australian Federal Police must also be satisfied that disclosure of the data would be appropriate in all the circumstances. Australia can make requests to any country and receive requests from any country. Sections 180A, 180B, 180C, 180D and 180E of the TIA Act govern authorisation of

	disclosure of telecommunications data from a domestic service provider in relation to enforcement of the criminal law of a foreign country. The TIA Act permits the Australian Federal Police to disclose telecommunications data to foreign law enforcement agencies on a police-to-police basis. The disclosure of existing data on a police-to-police basis is permitted only where the Australian Federal Police are satisfied that: - the disclosure would be reasonably necessary for the enforcement of the criminal law of a foreign country - any interference with the privacy of any person or persons that may result from the disclosure is justifiable and proportionate, and - the disclosure is appropriate in all the circumstances. Information disclosed on a police-to-police basis must only be used by the foreign country for the purposes for which it was requested, and the foreign country must destroy the information when it is no longer required for those purposes.
Bosnia and Herzegovina	**Brcko District of Bosnia and Herzegovina - The District Police - Crime Investigations Police** Article 72a of the Code of Criminal Procedure of the Brcko District of BiH on the issuance of the court order to a telecommunications operator or the other legal entity providing telecommunications servicesstipulates that it is lawful for the Police to send a direct request for acquisition of information about the user of a certain device or about the identity of a user's IP address, and such data are considered as legally valid evidence in the court proceedings. However, in order to legally obtain the data on the traffic and its content,and use them asa valid evidence in the court proceedings, it is necessary to conduct such evidence collection upon an order issuedby the court. Bearing in mind the above stated, we've created our policies and practices in sending the requests directly to foreign police agencies, prosecutors' offices and the courts. When consideringourprevious experience withsuch matters, the foreign police agencies used Interpol to provideus with the information about the identity of a person assigned the specific IP address that is linked to a crime within the competence of thePolice Investigation Unit of the Brcko District. **Federal Ministry of Internal Affairs** In the majority of cases, the requests are delivered to the foreign police agencies via NCB Interpol, and at the same time the competent Prosecutor's Office obtains and deliver the Application/Request for providing the international legal support; the timeframe for delivering the responses are individual for each separate country;
Bulgaria	If the needed data (subscriber, traffic or content data) has to be used in court as a valid and acceptable evidence, it has to be obtained through the mutual legal assistance channels, and has to be obtained by a prosecutor or a judge. Unfortunately this has proven to be very slow and inefficient. Police-to-police cooperation information is on the other hand easier and faster to obtain. Bulgarian law-enforcement authorities are allowed to request subscriber, traffic or content data from foreign law-enforcement authorities based on the international cooperation rules. There are no regulations regarding direct contact to a foreign service provider.
Canada	Direct requests to such entities typically occur in a limited range of circumstances. One situation reported by a number of divisions within the federal law enforcement agency (the Royal Canadian Mounted Police) was in joint investigations with a foreign law enforcement agency which yields timely results. The only other direct requests (with the exception of MLAT requests) occurred in exigent circumstances.

Croatia	Sending subscriber, traffic or content data request to a foreign police agency is usually not possible since in vast majority of the Convention on Cybercrime parties police authorities are not empowered to collect such data without an order from competent judicial authority. The execution of request sent to a foreign court or prosecution office would depend on which country is in question.
Czech Republic	In general MLA request is sent, however in some cases the foreign provider maybe approached via several other means such as: directly (eg. Facebook, Google, Microsoft); via particular law enforcement channel; via court order; or via emergency request. Other possibility is also request on basis of bilateral agreement on police or legal assistance (for CZ this is possible for example with the Slovak Republic).
Finland	Our policy is to follow the ways of mutual legal assistance. The element of control of authorities of both states is important. It is also a question of fundamental rights subject to safeguards and lawful procedures. The rules of the requested state have to be respected and the law enforcement authorities of the requesting state can´t request more than they could do or request in their own state. A request directed to Finland has to be sent to the competent authority. In this context it's however important to create swift and, within the limits of above-mentioned, lighter ways. This should be done by improving mechanisms based on international instruments on mutual legal assistance or other cross-border cooperation (for example by ensuring that there are on-call arrangements and/or developing notification procedure or otherwise based afterward control for particularly urgent situations) to change information depending on the nature of the measure and information in question. It´s conceivable to develop lighter regimes to measures like ordering subscriber information which are not so tightly related to fundamental rights and are not behind the consent granted by the court. As concerning the United States, a number of ISPs has decided to provide services to foreign law enforcement. It is a matter of voluntary discloser of data. Thus the principle of reciprocity is excluded. The US Department of Justice has accepted the co-operation and is encouraging to use these channels always when possible. In fact, there are no other options available. Often the subscriber and logging details are needed to better justify a search and seizure in a request for legal assistance to the USA with the view to obtain content data. Without direct provision of subscriber and logging details from ISPs, it would often be necessary to address two sequential requests for legal assistance to the United States with the view to obtain content data. Except in emergency request cases, the ISPs in the United States provide details of customers who are located in the EU, EFTA or ETA, only. In February 2015, Microsoft Corp. decided to limit disclosure of customer information further to where the company is able to confirm that the individual is located within the country requesting the information. Exceptions may, however, be granted when justified with additional information. Microsoft also requires that the maximum penalty of the offence is question has to be at least two years imprisonment. The statistics in the transparency reports of the ISPs in the United States clearly demonstrate the high volume of international direct requests. It would be impossible to channel these requests via traditional judicial or police channels. The most significant advantage is the response time. As concerning a regular request the response time is usually 1-2 weeks, but if urgent, from few hours to one working day. As concerning an emergency request, the response time is from 30 minutes to few hours. One of the ISPs has a specific portal for law enforcement requests. Via

	that portal prevention of data can be completed immediately. As concerning Finnish police authorities, a national point of contact (NCP) system is applied. This is also what the ISPs prefer. Thus the ISP can ensure that a request origin from a competent authority, and can also more easily inform of topical matters or changes concerning their services. We apply our quality system for international police and judicial co-operation concerning the ISPs, too. Thus all requests are subjected to a centralized legal control and operational appropriateness control, and are properly recorded in our diary for international correspondence. Consequently, our requests to a foreign ISP can easily be audited when needed. The current situation we have with Canada and Kik Inc, demonstrates a converse situation to the one with the USA. In January - June 2014, the Canadian company KIK Inc. was able to provide us directly subscriber information. Usually we obtained the data within one working day. After a Supreme Court decision (Citation: R. v. Spencer, 2014 SCC 43, Date: 20140613, Docket: 34644) the situation changed and MLA-requests are required for obtaining even subscriber details. As Canada has signed (23 Nov 2001) and ratified the Convention on Cybercrime in July 2015 and it came in force as late as on 1 Nov 2015, and there was no other applicable convention between our countries for the purpose, Canada required 'ad hoc' agreements between our countries in regard to our request for legal assistance. Several requests have been addressed to Canada, but not even the first one, which was made more than a year ago, has been finalized. As the Finnish ISPs keep their logs for one year only, the corresponding logs for identification of offenders and victims are lost. Keeping in mind that the cases in most requests concern sexual abuse of children, the non-existing cooperation with a foreign ISP demonstrates a miserable failure of international cooperation and in which the victims are minors.
France	Dans le cadre de la coopération internationale policière (canaux Europol, Interpol, G7 H24-7), seuls les éléments recueillis hors d'un cadre coercitif peuvent être communiqués aux services de police ou de justice étrangers. Ces données divergent en fonction des pays (cf rapport T-CY(2014)17 / décembre 2014). Pour tout autre sollicitation (demande de récupération de contenus...), les outils de coopération judiciaire internationale (Demande d'Entraide Pénale Internationale) sont les seuls d'usage.
Germany	The manual information procedure according to section 113 of the Telecommunications Act allows service providers only to release subscriber information to the competent bodies named in section 113 subsection (3). These bodies are the (domestic) responsible authorities for the prosecution of criminal or administrative offences, the (domestic) responsible authorities for averting danger to public safety or order and the (domestic) federal and state authorities for the protection of the Constitution, the Federal Intelligence Service and the Federal Armed Forces Counter-Intelligence Office. It is statutorily regulated in section 113 subsection (2) sentence 1, that information is not allowed to be delivered to other public or non-public bodies. In practice, German service providers do not comply with requests of foreign authorities. In its latest transparency report the Deutsche Telekom AG clarified, that

	requests of foreign authorities are not answered due to the sole responsibility of the national authorities. According to the transparency reports of smaller service providers, foreign authorities did not submit any requests in the relevant period (2014).
Hungary	Practices and policies are diverges. Officially our authorities use procedural MLA. Since this channel usually not functioning in a satisfactory way they often find themselves in an unfortunate situation. Sometimes Hungarian authorities try to get direct contact with the concerned service provider or do nothing. Service providers are also handling these cases in different ways. Some of them give IP addresses and entering dates sometimes registration data of the subscriber, but nothing else.
Italy	We have direct cooperation with some ISPs in the United States (Facebook, Google, Microsoft), which sent us directly and voluntarily subscriber information and (in some cases) traffic data too on a production order issued by the Public Prosecutor. For content data we use MLA procedure.
Japan	In principle, Japan's authorities request data from foreign service providers under a framework of International Assistance in Investigation. Yet, there is a case that we receive necessary data from foreign service providers within a scope of domestic investigation.
Latvia	"Cloud" service provider only provides its services within the territory of the Republic of Latvia (not within a Latvian section of the global network) when mentioned service provider is appropriately registered in the Republic of Latvia. Production order may be given directly to the service provider only if a service provider is registered within the territory of Latvia and in strict abidance to Latvian legislation. Rights and responsibilities of a service provider are listed in Electronic Communications Law of the Republic of Latvia (document may be found in attachment to this letter). Electronic Communications Law also regulates volume and procedure of information exchange between service provider and law enforcement organizations in the Republic of Latvia. Requests to foreign law enforcing organizations are being sent with the help of rogatory letter and in accordance to legislation of the republic of Latvia. Within Latvian territory, information is being received on the basis of Cabinet Regulation Nr.820 "Procedures by which Pre-trial Investigative Institutions, Bodies Performing Investigatory Operations, State Security Institutions, Office of the Prosecutor and Court Request and a Merchant of Electronic Communications Transfers Data to be Retained, and Procedures by which Statistical Information regarding Requests of Data to be Retained and Issuing thereof is Compiled" (document may be found in attachment to this letter). See attached laws
Lithuania	As a general rule, in order to obtain information in a criminal investigation or proceeding, we use MLA procedure, as set out in Section IV of the Criminal Procedure Code of the Republic of Lithuania "International Cooperation between Courts and Public Prosecutors of the Republic of Lithuania and Foreign Entities and International Organisations". However, Art 66 Para 2 of this Section also envisages the possibility for Lithuanian courts, public prosecutors and pre-trial investigation entities to submit requests to foreign entities and international organisations directly. Besides, as mentioned before, there are no legal prohibitions as regards the addressee of a domestic production order, meaning that public prosecutor is allowed to deliver the resolution (domestic production order) envisaged by Art 155 of the CPC to the service provider irrespective of whether it offers its service on the territory or

	outside of Lithuania. Such production order may be used to obtain basic subscriber information and traffic data (access logs). For the purposes of obtaining content data, search and seizure procedures on the basis of Art 145, 146 and 149 of the CPC. Since this is a more intrusive procedural measure, MLA procedure is used and requests are sent via prosecutor's office to a competent authority of a foreign country.
Luxembourg	(a)Nous estimons qu'il est utile que les fournisseurs de service répondent directement à des demandes concernant les données relatives aux abonnées (BSI = Basic Subscriber Information) si les conditions indiquées ci-dessus sub 1.c. sont données. Nos services de police sont habilités à adresser de telles demandes directement aux fournisseurs de services étrangers. D'après nos expériences, si les conditions indiquées ci-dessus sub 1.c. sont données, et si le fournisseur de services a pu vérifier qu'il s'agit bien d'un service de poursuites de l'Etat (au moyen de la vérification de l'adresse électronique) qui en a fait la demande, les données relatives aux abonnées sont fournies sans problème. (b) et (c) Nous estimons que ces données sont des données plus sensibles qu'il faut protéger plus pour garantir au maximum le respect de la vie privée. En conséquence, la remise de ces données doit être subordonnée à l'émission d'un mandat judiciaire et d'une commission rogatoire internationale le cas échéant. Nos demandes relatives aux données de trafic et de contenu sont toujours faites au moyen de mandats du juge d'instruction et de commissions rogatoires internationales. De même nous exigeons des autres Etats les mêmes actes formels pour obtenir ces données d'un fournisseur de services luxembourgeois.
Mauritius	Either by way of a Judge's order;or By Mutual Legal Assistance procedure
Moldova	According to our law and practice the police service can request foreign police agency to help them with providing information on cybercrime cases but this information is obtained by carrying out operational investigative measures and will not be considered as evidence on a criminal case. Thus, the General Prosecutor's Office addresses MLA requests to foreign prosecution service or to the Ministry of Justice of the requested state in case this is the competent authority where the requests should be sent. We do not directly request the service providers to offer the needed informational data
Monaco	
Montenegro	Competent authorities in Montenegro so far have always been using the Mutual Legal Assistance requests.
Netherlands	Please see the answer to question 1c.
Panama	Higher Special Prosecutor's Office for Crimes against Intellectual Property and Information Security maintains no direct cooperation with Foreign Service providers. Requests are made through Mutual Legal Assistance, based on an agreement, treaty or reciprocity. Policies, experience and practice concerning requests for subscribers information or

	traffic and content data from a foreign agency have always been done through judicial assistance.
Philippines	Sections 13-15 of the CPA-IRR provides the policies regarding direct requests for subscriber, traffic, and content data. Section 13 provides that a court warrant shall be secured before law enforcement officers and/or service providers can collect or record, by technical or electronic means, computer data that are associated with specified communications transmitted by means of a computer system. The court warrant requires a written application, and the examination under oath or affirmation of the applicant and the witnesses he may produce, and the showing that: (1) there are reasonable grounds to believe that any of the crimes enumerated hereinabove has been committed, is being committed or is about to be committed; (2) there are reasonable grounds to believe that the evidence that will be obtained is essential to the conviction of any person for, or to the solution of, or to the prevention of any such crimes; and (3) there are no other means readily available for obtaining such evidence. To compel disclosure/submission of subscriber's information, traffic data or relevant data in a person's/service provider's possession or control, law enforcement officers are also required to secure a court warrant. The law enforcement officer can order the person or service provider to disclose or submit, within seventy-two (72) hours from receipt of such order, in relation to a valid complaint officially docketed and assigned for investigation by law enforcement authorities, and the disclosure of which is necessary and relevant for the purpose of investigation. (Section 14, CPA-IRR) Further, when a search and seizure warrant is properly issued, the law enforcement authorities shall likewise have the power to conduct interception within the time period specified in the warrant, and to: (1) search and seize computer data; (2) secure a computer system or a computer data storage medium; (3) make and retain a copy of those computer data secured; (4) maintain the integrity of the relevant stored computer data; (5) conduct forensic analysis or examination of the computer data storage medium; and (5) render inaccessible or remove those computer data in the accessed computer or computer and communications network. (Section 15, CPA-IRR)
Portugal	As said above, Portugal acquired some practise requiring information to some service providers based in the United States. Informal agreements have been established and template forms have been agreed. All the concerned providers agreed voluntarily provide certain types of information. This agreement was achieved only regarding requests that respect, both the Portuguese and the American regulations at this respect. In other words, the providers just accept requests and provide information if the request is issued according to the Portuguese law and also respects the American regulations.
Romania	Subscriber information, traffic data and content data is obtained through MLA. Subscriber information can be requested through the police cooperation channels, however the answer depends on the legislation of each country.
Slovakia	Prosecutors require data only for the evidential purposes. Therefore, such data are requested exclusively from competent authorities of the requested states on the basis of requests for mutual legal assistance (in number of cases a request for expedited preservation of data precedes the request for mutual legal assistance; however, such request is also sent by prosecutors to the competent authorities, not

	directly to foreign service providers). The purpose of the request determines the mutual legal assistance as the only way of obtaining evidence admissible in the court proceedings. Same procedures are applied for different kind of data.
Slovenia	We have only few practices and experiences – in some cases court issued a court order, which was translated and directly sent to service provider (i.e. facebook, skype). But usually requests are send via Europol, this is our official way.
Spain	So far and based in our experience, the large US companies usually address –without processing International Letters Rogatory- the requests for direct information from Spain on data relating to subscribers made –in any case- through judicial order as provided for in our domestic law. As mentioned above, after the entry into force of the procedural reform and more specifically of the new article aforementioned (588 ter m), the judicial authorization to obtain subscribers information is not required in Spain but the request can be directly made either by the Public Prosecutor or the Judicial Police. We are eager to see which criterion shall be followed by these companies when requests are to be made in that manner, that is to say, without judicial authorization since at present, we lack experience in relation to this matter.
Switzerland	National ISP do not comply with direct formal requests from foreign prosecuting authorities. Instead, national MLA and police authorities (single point of contact and co-ordination) provide for possibilities of expedited procedures for providing subscriber or traffic data.
Tonga	In this scenario, Tonga would make the request through the Attorney General under the Mutual Assistance in Criminal Matters Act 2000 and the Foreign Evidence Act 2000 to the specific agency.
Turkey	The information acquired from foreign countries by the local law enforcement can be used intelligence purposes only. Courts can verify the information by sending a judicial rogatory to the related country. Official letters sent by the courts which ask for the subscriber, traffic and content data are received to be sent foreign countries. Generally, this kind of requests are evaluated by them and according to their laws, they notify us wheter they could provide the requested data or not.
United Kingdom	For evidential purposes this almost always has to be done by way of Letter of Request, which does not always elicit a response. Speediness of response is dependent on individual requested territories. Informal requests for intelligence can be made, but success rates vary. Routes are either direct to provider or via the relevant International Liaison Officer. In terms of our practices because the police are the investigator we would expect them to make an initial request for data to be preserved. Where they know the CSP will respond to a RIPA notice then we would expect them to serve such a notice without any Crown Prosecution Service involvement. If a formal request is required then we would submit the Letter of Request either directly to a prosecutor or court or via the UKCA as appropriate.
United States	- In routine or emergency cases, the US can make direct requests to providers in some foreign countries for different categories of data, depending on what the foreign country's law permits. We do not have enough experience to characterize this. - In routine cases, US law permits other countries to request voluntary disclosure of subscriber and/or traffic data directly from US providers without notice to the US. Major US providers usually require the requesting country to provide them

	the legal document that would be valid in the requesting country. At least one major US provider rejects this process per se. The process is often unsuccessful and the trend is to diminishing cooperation. - In cases involving a threat to life or of serious physical injury, US law permits the US and other countries to request voluntary disclosure of subscriber, traffic, and content data directly from US providers. The process is often unsuccessful and the trend is to diminishing cooperation. If the US providers disclose content to foreign countries, it must be routed (briefly) through the US government.

b. What are your practices and experiences regarding criminal or non-criminal emergency requests?

Australia	The AFP Operations Coordination Centre (AOCC) Watchfloor are required to undertake emergency requests afterhours that are classified life-threatening. A life threatening communication is one which gives a person reasonable grounds to believe that there is a serious and imminent threat to the life or health of a person and may include events such as: - a person being seriously injured or making threats of self-harm - a bomb threat - an extortion demand - a kidnapping, or - response to calls from vessels in distress. These requests are submitted in accordance with the Telecommunications Act 1997 and the TIA Act. Afterhours requests from Foreign Law Enforcement Agencies are directed through INTERPOL. When the official request has been received results will be disseminated back through INTERPOL. Any other urgent requests that do not fall within the above parameters are actioned accordingly during business hours.
Bosnia and Herzegovina	**Brcko District of Bosnia and Herzegovina - The District Police - Crime Investigations Police** We do not have any practices or experience relating to criminal or non-criminal emergency requests. Article72aof the Law on Criminal Procedure of Brcko District of Bosnia and Herzegovina in its paragraph (2) stipulates that in urgent cases the Prosecutor may order to a telecommunications operator or the other legal entity providing the telecommunications services to provide them with information on the relevant person's use of telecommunication services where such obtained information a resealed until the issuance of a court order. Prosecutor immediately informs the court on the measures taken so the court can issue its order within72 hours. In case the court omits to issue an order, the Prosecutor returns such information without accessing it. **Federal Ministry of Internal Affairs** Regarding the urgent requests, the focal point 24/7 is used, regarding the cases of cybercrime. Our experience in this regard have been positive so far. Further, when it comes to specific internet service providers aboard – we use on-line application for obtaining data, which is also followed by the Application/Request for providing the international legal support.
Bulgaria	
Canada	Service providers are often but not always cooperative in an emergency situation. Most police agencies contacted (which extended to the divisions of the Royal Canadian

	Mounted Police) reported that all service providers, whether domestic or in the United States, have provided subscriber information or IP addresses upon request in emergency situations. Respondents noted that all required specific forms to be completed to obtain the information but that all the companies cooperated in a timely fashion. Legal counsel further noted in addition that companies do not incur legal liability if they cooperate on a voluntary basis where no legal impediment to such cooperation exists. Section 487.0195(2) of the Criminal Code expressly indicates that providers do not incur civil or criminal liability if they preserve data or provide a document to law enforcement when they are not prohibited by law from doing so, which would include law enforcement requests made under emergency (exigent) circumstances.
Croatia	In urgent matters, Croatian authorities as a rule use the institute of expedit preservation of data from Art 16 of the Budapest Convention, successfully. Subsequent letter rogatory will be sent via fax, e-mail etc. to the extent that such means provide appropriate levels of security and authentication. Please note that we do not have a developed practice regarding the content data requests.
Czech Republic	Czech criminal justice authorities deal only with requests issued within criminal proceedings; therefore, there is no experience with "non-criminal emergency requests". All requests for subscriber, traffic and/or content data coming from designated foreign judicial authorities are considered requests for mutual legal assistance (MLA requests), as such, they shall be addressed to Czech executing judicial authorities. Foreign judicial authorities may send the MLA requests directly to Czech judicial authorities if an international agreement provides for such a possibility. Most frequently the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union is used as grounds for that kind of direct contact. In urgent cases, MLA request may be sent first by electronic means and its execution may begin immediately. However, Czech service providers are entitled to provide subscriber, traffic and/or content data exclusively to authorities listed by the Act on Electronic Communication (Act. No. 127/2005 Coll., Article 97). The Law does not mention any type of foreign authorities which means they have to follow the process of MLA requests in all cases they need the above mentioned data. Finally, there are subjects offering electronic communication services which do not fall under the Law on Electronic communication – typically some of "freemail" providers. They do not have data retention duties but they often store the data for commercial purposes. In case such a provider "offers services in a territory" outside the Czech Republic and needs no assistance from Czech authorities, foreign judicial and law enforcement authorities may contact such a provider in that state on the grounds of their national law. The Czech Police adds that all requests were settled promptly and without any difficulties.
Finland	Emergency request are relatively rare but often extremely important. Criminal requests refer usually to severe cases of menace such as bomb threats, threats of school shootings, and kidnappings. Non-criminal requests refer usually to severe suicide threats and missing person cases. We have applied both forms of emergency requests.

	We have experienced outstanding service from the concerned foreign ISPs. The response time is depending what type and how much information is needed, and in how many systems the concerning ISP need to look for it. The response time is always very short, as best 30 minutes and at the most few hours, only. The response time is much more shorter than any traditional police or judicial procedure can ever demonstrate, and is meeting the actual operational need for the information. As conceding our practices, we apply a centralized handling of all requests to foreign ISPs and are able to send an emergency request on a short notice.
France	Concernant les FSI français, le traitement des réquisitions judiciaires est amélioré par l'existence de points de contact dédiés au sein des entreprises ; ceux-ci sont alors systématiquement sollicités afin d'accélerer le traitement d'une demande urgente. Dans le cadre d'urgence vitale, les dispositions de l'article 223-6 du Code Pénal sont rarement rappelées aux FSI. Concernant les FSI étrangers et plus particulièrement américains, les notions de « Terrorisme » et «sauvegarde de la vie humaine vitale » définissent généralement la notion d'urgence vitale. Dès lors, en raison du péril imminent, les FSI, signataires des conventions d'entraide et après avoir été informé des faits en cours, sont sollicités directement par les enquêteurs. En dehors de cette définition d'urgence vitale, les enquêteurs peuvent toutefois solliciter des informations auprès des FSI selon une procédure particulière : Le service demandeur prend attache avec le Guichet Unique (présent au sein de la DCPJ/SDLC/OCLCTIC du Minsitère de l'Intérieur) et expose ses arguments relevant de l'urgence (ex :mesure de garde à vue en cours). Après validation par le GU du caractère d'urgence, un numéro de validation est assignée à la réquisition judiciaire transmise au FSI. Fort du partenariat entre le Ministère de l'Intérieur et les FSI, ce numéro de validation permet à la société sollicitée d'identifier la demande comme urgente et de la traiter comme telle. Cette réquisition est également transmise au point de contact dédié du GU afin de veiller à l'application du protocole.
Germany	In non-emergency cases the information request must be submitted to the service providers by the (domestic) competent body in textual form with the regulation that allows the collecting of data explicitly named (section 113 subsection (2) sentence 1 of the Telecommunications Act). According to sentence (2) of section 113 subsection (2) of the Telecommunications Act the request can in exigent circumstances also be submitted formally different, e.g. verbally or by phone. In this case, the request has to be subsequently confirmed in textual form without undue delay, sentence (3) of section 113 subsection (2) of the Telecommunications Act. These regulations refer to criminal and non-criminal emergency requests equally. In case of outgoing emergency requests (requests by German authorities to foreign service providers) our experience has shown that service providers usually request proof of imminent danger to life (screenshot, link - among others). In case the foreign service provider considers it possible to voluntarily comply with the disclosure request, the data is provided to the requesting authorities, usually within a short time frame. Most providers disclose subscriber data and/or login IP addresses. This procedure mostly applies to US-based service providers.
Hungary	We could not express exact practice. However we would like point out here that in case of emergency answer usually arrives. Some service providers have special emergency request policy or form and we find them really useful for both side. In case of an urgent request LEAs send a preservation request before MLA through COE 24/7 or G8 24/7 channel to LEA partners in other States.

Italy	Our experience is limited to criminal cases: we have direct cooperation with some ISPs in the United States (Facebook, Google, Microsoft), according to their policies.
Japan	By considering contents of such request individually and specifically, police, in principle, respond as with above-mentioned response. With regard to general proceedings concerning for a provisional remedies before the merits of civil suits, Civil Provisional Act governs civil provisional remedy proceedings. However, there exists no rules regarding a mechanism of requesting disclosure of information of senders to domestic and foreign service providers in Civil Provisional Act . We don't know whether there exist any legal frameworks for the disclosure between the court and any foreign service providers.
Latvia	"Cloud" service provider only provides its services within the territory of the Republic of Latvia (not within a Latvian section of the global network) when mentioned service provider is appropriately registered in the Republic of Latvia. Production order may be given directly to the service provider only if a service provider is registered within the territory of Latvia and in strict abidance to Latvian legislation. Rights and responsibilities of a service provider are listed in Electronic Communications Law of the Republic of Latvia (document may be found in attachment to this letter). Electronic Communications Law also regulates volume and procedure of information exchange between service provider and law enforcement organizations in the Republic of Latvia. Requests to foreign law enforcing organizations are being sent with the help of rogatory letter and in accordance to legislation of the republic of Latvia. Within Latvian territory, information is being received on the basis of Cabinet Regulation Nr.820 "Procedures by which Pre-trial Investigative Institutions, Bodies Performing Investigatory Operations, State Security Institutions, Office of the Prosecutor and Court Request and a Merchant of Electronic Communications Transfers Data to be Retained, and Procedures by which Statistical Information regarding Requests of Data to be Retained and Issuing thereof is Compiled" (document may be found in attachment to this letter). See attached laws
Lithuania	So far we had only few criminal emergency requests involving foreign service providers, mainly related to tracing missing people or to imminent threat of a serious crime to be committed. The requested information has been disclosed by foreign service providers within the time range somewhere between 30 minutes to 2 days. Such emergency requests call for a clear description of the emergency situation, especially if they are not immediately accompanied by the necessary court sanctions.
Luxembourg	Il faut d'abord définir l'urgence : L'urgence en cette matière n'est donnée que s'il y a « vie en danger » (life in danger) ou danger imminent de perte/destruction des données. Dans le deuxième cas le législateur luxembourgeois est intervenu et a prévu dans un nouvel article 48-25 du code d'instruction criminelle la conservation rapide des données informatiques pour une période de 90 jours (freezing order). Cette procédure simplifiée qui permet de geler les données en attendant les actes formels de procédure est communément utilisée en pratique et n'a encore rencontré aucun problème. Dans le premier cas, tous les fournisseurs de services ont des procédures spéciales en place qui permettent aux autorités étatiques (Police, Parquet, Tribunal) de les contacter en urgence et d'obtenir les informations disponibles (données relatives aux abonnées, de trafic et de contenu) et nécessaires en vue de prévenir le danger dans un délai extrêmement rapproché (10 à 30 minutes) sur base d'une simple requête motivée.

Mauritius	For emergency requests, the CERT-MU can remove the illegal, harmful or hacked account by making the request to Anti Phishing Working Group or Facebook. For phishing cases, the response is fast and positive. What is challenging is as regards Facebook. In one case, CERT-MU successfully applied to Facebook for the removal of the posting.
Moldova	As for the emergency requests, the practice we usually use is to first ask the foreign state by using our 24/7 contact point if they can help us with preservation of data, monitoring of traffic data, identification of subscriber etc. in order not to lose the information we need and then we send them the MLA request.
Monaco	La coopération directe avec les autorités judiciaires étrangères se fait sur le fondement de la Convention européenne d'entraide judiciaire en matière pénale en date du 20 avril 1959 ratifiée par l'ordonnance souveraine n°1088 du 4 mai 2007 pour les pays membres du Conseil de l'Europe ou parfois par des demandes directes de la Direction de la Sureté Publique à ses homologues étrangers à propos de la pédopornographie par exemple. Certains Etats comme le Canada acceptent cette coopération directe entre services de police sans aucun support conventionnel. Quel que soit le rapport juridique, il apparaît que cette coopération donne des résultats inégaux selon les Etats et les fournisseurs de services numériques
Montenegro	No experience
Netherlands	Emergency requests can be asked for. Because the ISP in such circumstance will give out the information on a voluntary basis, the ISP will first assess themselves: 1.Is this an emergency situation? 2.Is there an actual threat? 3.Does the situation pose an imminent danger or life or physical wellbeing? Dutch law enforcement and judiciary will file – again via the SPOC – a request to meet those criteria. If later on the information is to be used in a criminal case, often MLA is needed.
Panama	Until now, in Panama we have not experienced this practice or experience. Attempts have been made to establish communication lines or channels to gain information informally, but it has not yet been able to implement (Ex. Red 24/7 of G8)
Philippines	Emergency requests are usually limited to criminal cases though there is limited experience on this.
Portugal	There is no enough experience at this respect.
Romania	Our experience is limited to criminal cases. Romania has a direct cooperation with Google, which sent us directly and voluntarily subscriber information (only) based on direct requests. We have also direct cooperation with Western Union, which provides directly information related to transactions.
Slovakia	As regards requests for expedited preservation and partial disclosure of traffic data

	(Art. 17 of the Budapest Convention), these requests may be sent via 24/7 channels (National Interpol Bureau). The same applies to urgent requests for mutual legal assistance in criminal matters.
Slovenia	We also have rare cases regarding emergency reguests, so it's hard to describe any good practices or experiences. We would probably use police liason officer or police attaché for emergency cases with the help of Sector for international police cooperation.
Spain	
Switzerland	The specific practice varies, depending on the requesting authority involved and the requested data holder. Often, in cases of outgoing emergency request (mostly to the US), requests are being handled on a pragmatic level. The practice regarding incoming emergency requests from abroad is not fully developed.
Tonga	The agency is normally contacted via email or telephone through informal means. The agency is then told that the formal request will follow shortly.
Turkey	Generally, if it is considered as emergency request, 24/7 Point of Contact is considered as the fastest method to notify foreign counterparts. Most likely, due to the nature of the emergency request, foreign counterparts provide what is asked, if possible.
United Kingdom	Some CSPs will accept direct requests from UK law enforcement. Generally this is confined to subscriber and traffic data. In the US Google, Facebook, Twitter and Microsoft will provide information in emergency situations which involve danger or serious physical injury to any person. They will also provide information where: - the provider obtains knowledge or facts or circumstances from which it is apparent that a recent offence involving indecent images of children has been committed using the services of the provider and there is immediate danger of serious physical injury to any person; - the subscriber consents to the data being disclosed; - the subscriber is deceased, his or her next-of-kin consent to the data being disclosed; - the provider operates a "voluntary disclosure" scheme in accordance with UK law (i.e. a RIPA Request), the offence is serious (e.g. indictable offence), and there are no freedom of speech issues. However, Crown Prosecution Service experiences are mixed. We sometimes obtain what we want in a timely fashion though sometimes do not. It will often depend on the cooperation of the owners of the server, and also on the nature of the data held. In the case of criminal emergency requests, there is much greater cooperation. Assistance is usually limited to intelligence – the formal route has to be followed for evidential material. On the whole, foreign authorities, particularly in EU countries who have agreed to direct transmission of evidence have been helpful. It is often the case however that it will take some time for the data to be received in evidence when it is requested via a Letter of Request. In addition it can also be the case that it is difficult to obtain electronic data from a server even when it is requested on an urgent basis via LOR and the requested country agree to co-operate, where the owners of the server are not cooperative.
United States	See above. Our overwhelming experience to date is with criminal cases. Emergency requests that are clearly non-criminal are extremely rare.

Q 3. Would you have comments on other question raised in the Discussion Paper prepared by the Cloud Evidence Group?

Australia	No input.
Bosnia and Herzegovina	We do not have any comments to the other questions raised in the Discussion Paper of the Cloud Evidence Group.
Bulgaria	
Canada	No additional comments at this time.
Croatia	
Czech Republic	
Finland	
France	La définition du concept de propriété de la donnée et du droit applicable sont primordiaux. Doit-on considérer que les données sont situées au siège de l'entreprise FSI? Au sein de sa succursale dans un pays de l'UE ? Dans le(s) pays d'implantation des serveurs ? Quid du hachage des données entre différents serveurs de l'opérateur répartis sur différents territoires ? Plus généralement, il serait également peut-être opportun de s'interroger sur l'Etat qui serait légitime pour assurer la protection des données personnelles d'un individu (et ainsi être à même d'en autoriser la communication à une autorité étrangère) : Est-ce l'Etat sur le territoire duquel les données sont stockées ? Est-ce l'Etat dont l'individu a la nationalité ? Est-ce l'Etat de résidence effective de l'individu. Ainsi, la récente position de la CNIL allemande quant au nécessaire hébergement en Europe des données personnelles des ressortissants européens est intéressante.
Germany	Germany has no further comments on other question raised in the Discussion Paper prepared by the Cloud Evidence Group.
Hungary	In our opinion it would be very useful for all parties if we could come out a common policy on handling these data in order to avoid breaching any legal norm.
Italy	Italy participates in the Cloud Evidence Group.
Japan	None.
Latvia	
Luxembourg	
Mauritius	Retention of data by service providers. The length of the retention???
Moldova	We don't have any questions.
Monaco	
Montenegro	
Netherlands	
Panama	With regard to testing in the cloud, Panama must deepen an arduous training on this subject, to gain experience; we still do not have experience in this kind of practice.
Philippines	We concur and support all items covered in the Discussion Paper.

Portugal	No
Romania	Romania participates in the Cloud Evidence Group.
Slovakia	The cloud computing, jurisdiction, principle of territoriality and technical issues (such as encryption) and issues related to mutual legal assistance in criminal matters are relevant and require further examination. Currently, the main issue is, however, the data retention. Without effective data retention, no data or only limited data are available. Current situation limits the international cooperation.
Slovenia	
Spain	
Switzerland	
Tonga	No
Turkey	
United Kingdom	
United States	No comments.

Appendices

Laws of Latvia

- Electronic Communications Law
- Procedures by which Pre-trial Investigative Institutions, Bodies Performing Investigatory Operations, State Security Institutions, Office of the Prosecutor and Court Request and a Merchant of Electronic Communications Transfers Data to be Retained, and Procedures by which Statistical Information regarding Requests of Data to be Retained and Issuing thereof is Compiled

Questionnaire

www.coe.int/TCY

Strasbourg, 5 October 2015 T-CY (2015)21 E

Cybercrime Convention Committee (T-CY)

Cloud Evidence Group

Criminal justice access to electronic evidence in the cloud

Questionnaire in preparation of the hearing on 30 November 2015

Background:

The T-CY in December 2014 established the "Cloud Evidence Group" tasked to explore solutions on criminal justice access to evidence stored on servers in the cloud and in foreign jurisdictions, including through mutual legal assistance.

In June 2015, the Cloud Evidence Group submitted to the T-CY a discussion paper on "Challenges".

On 30 November 2015, that is, prior to the 14th Plenary of the T-CY (1-2 December), the Group will hold a hearing for service providers. The hearing is to focus on the following specific issues:

- When is a service provider considered to be "offering a service on the territory" of a Party in the sense of Article 18.1.b Budapest Convention? And thus, when is a service provider subject to a domestic production order for subscriber information?

- Are, and if so, when do service providers respond directly to requests from foreign criminal justice authorities? What are their policies, practices, conditions and specific format and requirements for responding directly to a request for (a) subscriber, (b) traffic, and (c) content data? What are their policies, practices and procedures regarding criminal or non-criminal emergency requests?

The Cloud Evidence Group, in its meeting on 27 and 28 September 2015, came to the conclusion that in order to obtain a full understanding of these issues, Parties and Observer States are invited to share the experience and practices of their criminal justice authorities.

Parties and Observer States are invited to submit their responses in English or French in electronic form no later than **10 November 2015** to marie.agha-wevelsiep@coe.int.

The replies will be treated as restricted and will not be published.

Questions

Question 1: Domestic production orders for subscriber information when "offering a service on the territory" of a Party

Considering Article 18 paragraph 1.b. of the Budapest Convention and its explanatory report (see appendix):

a. When do you, as a criminal justice authority, consider that service provider[2] is offering a service on your territory?

b. Thus, when do you consider that you can deliver a domestic production order for subscriber information directly to the service provider offering the service?

c. In your experience, what are the criteria, conditions or circumstances that make service providers accept or decline such a request?

Question 2: Direct cooperation between criminal justice authorities (such as police, prosecutors or courts) and foreign service providers

Transparency reports published by many service providers indicate that service providers often respond to request for data that they receive directly from criminal justice authorities. Thus:

a. What are your policies, practices and experiences regarding direct requests (a) subscriber, (b) traffic, and (c) content data to a foreign police agency, prosecution service or court?

b. What are your practices and experiences regarding criminal or non-criminal emergency requests?

Question 3: Would you have comments on other question raised in the Discussion Paper prepared by the Cloud Evidence Group?

[2] The Budapest Convention applies a broad concept covering all types of service providers:

Article 1 – Definitions
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.

Appendix 1: 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.

Appendix 2: Background documents

T-CY(2015)10 Criminal justice access to data in the cloud: challenges
http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b59

T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime,
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c

Terms of reference of the Cloud Evidence Group, http://www.coe.int/en/web/cybercrime/ceg

Conclusions of the Octopus conference 2015:
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680319026

Transborder Group: http://www.coe.int/en/web/cybercrime/tb

European Court of Justice, Google v. Spain:
http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf

Yahoo Case: http://www.stibbe.com/en/news/2014/july/benelux-ict-law-newsletter-49-court-of-appeal-of-antwerp-confirms-yahoo-obligation