www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Strasbourg, Version 25 October 2018 T-CY (2018)26

## Cybercrime Convention Committee (T-CY)

**Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime**

# Conditions for obtaining subscriber information in relation to dynamic versus static IP addresses: overview of relevant court decisions and developments

**Discussion paper**
**prepared by the Secretariat in cooperation with**
**T-CY members of the Protocol Drafting Group**

# Content



**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

# 1 The issue

Effective solutions for obtaining subscriber information have been the focus of the Cybercrime Convention Committee (T-CY) for several years given the importance of such information for criminal investigations.

In 2014, the T-CY carried out a survey on "rules on obtaining subscriber information" and in 2017, the T-CY adopted a "Guidance Note on Production Orders for Subscriber Information" under Article 18 Budapest Convention.

The T-CY Cloud Evidence Group in 2016 had also recommended differentiating between types of data sought:

- "Subscriber information", that is, information to identify the user of a specific Internet Protocol (IP) address or, vice versa, the IP addresses used by a specific person. Subscriber information also comprises data from registrars on registrants of domains.
- "Traffic data", that is, log files that record activities of the operating system of a computer system or of other software or of communications between computers, especially source and destination of messages.
- "Content data" such as emails, images, movies, music, documents or other files. A distinction should be made between "stored" content, that is, data already available on a computer system and "future" content that is not yet available and will have to be obtained in real time.

Additional solutions on obtaining subscriber information through direct cooperation with service providers and/or expedited mutual assistance are to be developed within the context of the negotiation of an Additional Protocol to the Budapest Convention.

However, in the light of several court decisions regarding the nature of subscriber information in relation to dynamic as opposed to static IP addresses, the T-CY Protocol Drafting Plenary in July 2018:

> Took note of relevant national and international developments, including court decisions and procedural rules, related to subscriber information, and the challenges of delineating categories of information and how they relate to each other, as well as the concerns expressed by some delegates with respect to increasing restrictions on the obtaining of subscriber information, and invited the Secretariat in cooperation with interested Parties to prepare a short working paper on the question of subscriber information related to dynamic and static IP addresses for the PDG meeting on 17-19 September 2018;

The present working paper considers whether subscriber information related to dynamic IP addresses should be considered traffic data or equivalent to traffic data, and thus whether rules for obtaining traffic data (and not rules for obtaining subscriber information) apply to dynamic IP addresses.

This is related to the broader questions of whether:

- there is a case for a lower threshold for obtaining subscriber information related to both static and dynamic IP addresses;
- restrictions for the retention of traffic data and access to retained data would also apply to subscriber information;
- the disclosure of subscriber information by a service provider interferes with data protection rights or also with the right to the secrecy of communications.

# 2 Traffic data und subscriber information in the Budapest Convention

## 2.1 Subscriber information related to static versus dynamic IP addresses

Subscriber information is the type of data most often sought by criminal justice authorities in criminal investigations of cybercrime and other cases involving electronic evidence.

Typically, what is needed is:

- IP address data related to a specific account, website or similar data used in a criminal offence. The IP address data includes the IP address used to create the account, the last login IP address or the IP address used at a specific moment in time;
- Subscriber information related to a specific IP address used in a criminal offence.

While a static IP address is stable and assigned to a specific subscriber for the duration of the service arrangement (similar to a telephone number) and while a service provider can look up such information in a database of subscribers, a service provider may assign an IP addresses to multiple users in a dynamic manner,[1] and a time stamp is needed to determine the subscriber to whom the IP address has been assigned at a specific moment in time.

For this, the service provider may need to look up or analyse traffic data of multiple users. According to the jurisprudence of some courts, this fact of looking up traffic data as such may be considered an interference with the right to private life and specifically the right to the secrecy of communications and not only an interference with data protection rules.

In this connection it should be noted that this looking up of traffic data to identify which IP address was assigned to a subscriber at a specific moment in time is likely to entail an automated query of databases by a service provider and not necessarily an analysis of traffic data.

Moreover, it would be misleading to state that a dynamic IP address – as opposed to a static IP address – is necessarily part of a concrete communication and on its own alters the degree of interference with the rights of individuals:

- A dynamic IP address may be assigned to a particular subscriber not for each new communication but, for example, for several days or months or until the subscriber resets the router.
- The device of a subscriber may automatically connect and use an IP address without the subscriber engaging in an active communication, for example, for updates even while the computer is idle or to reconnect to a new cell site when moving. Thus, devices communicate with each other without human agency and without involving substantive content.

The purpose of obtaining subscriber information in a criminal justice context – be it in relation to static or dynamic IP addresses – is the same, namely, to identify the subscriber of

[1] The reason for the dynamic allocation of IP addresses is that under Internet Protocol version 4 (IPv4), the available numbers are limited. This problem will eventually be resolved once the transition to IP version 6 has been completed or is more advanced.
A further complication is the large-scale Network Address Translator (NAT) architecture where one IP address may be assigned to hundreds of users. For a summary of this see section 5.4 of the T-CY Cloud Evidence Group report on "Criminal justice access to data in the cloud: challenges"

a specific account or website, or the subscriber of an IP address in relation to a specific criminal investigation where relevant information about the content, context or nature of the crime has been obtained by the investigating authorities already through other means.

## 2.2 Provisions of the Convention

The Budapest Convention contains definitions of "traffic data" and of "subscriber information":

> Article 1 d "traffic data" means any computer data relating to a communication by means of a computer system, *generated* by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.
>
> Article 18.3 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.

The Convention does not explicitly refer to Internet Protocol addresses as part of subscriber information but given the broad range of the definition of Article 18.3 (see also the Explanatory Report) and the reference to "access numbers", IP addresses may be considered to be included, if necessary to identify a subscriber.

In July 2018, the T-CY adopted a template for mutual legal assistance requests for subscriber information. While this template is to provide guidance and is not binding, the appendix listing details of information that may be requested, includes "IP address used for the initial registration of the accounts", "IP address used for the last access to the accounts", and "IP address used for access to the account in the period […]".

The Convention thus also does not refer to or make a distinction between static and dynamic IP addresses.

## 2.3 Rules for obtaining subscriber information in the Parties

In 2014, the T-CY carried out a survey on "rules on obtaining subscriber information".[2] The initial intention had been to prepare a Guidance Note on this question but given the diversity of rules, conditions and procedures, the information received from Parties was turned into a stand-alone report which was then adopted by the T-CY in December 2014.

The report showed that:

- In 12 Parties, subscriber information can be obtained through a formal police request. However, in three of these (Austria, Denmark and Slovenia) this applied only to static IP addresses, and an order of a prosecutor (Austria) or judge (Denmark, Slovenia) was required for dynamic IP addresses.

[2] 28 Parties replied to the questionnaire.

- In 8 Parties, subscriber information could be obtained through an order of a prosecutor.
- In 13 Parties, an order by a judge was required either always or – in some Parties – in some cases (e.g. dynamic IP addresses, information beyond basic subscriber information, information related to a specific communication and thus representing data falling under data retention rules).

The report concludes that:

> Most of the responding Parties indeed make a distinction in their definitions or concepts between "subscriber information" and "traffic data".
>
> However, the conditions for obtaining subscriber information are diverse:
>
> - In most of the responding Parties, the conditions for obtaining subscriber information appear to be the same or similar to those for obtaining traffic data, in particular if subscriber information is related to a dynamic IP address. In more than half of these Parties, obtaining subscriber information requires judicial authorisation, and in others a prosecutor or an authorised senior law enforcement officer can order the production of subscriber information.
> - In other Parties, the requirements for obtaining subscriber information are lower than those for traffic data, and the production of subscriber information can be ordered by the police or a prosecutor.
>
> In conclusion:
>
> - most Parties differentiate between subscriber information and traffic data;
> - in some countries, the interference with the rights of individuals is considered to be substantially different when obtaining subscriber information, including in relation to an IP address, in a specific criminal investigation on the one hand, and traffic data on the other;
> - consequently, in those countries, different rules should apply for obtaining such information;
> - conditions for obtaining subscriber information are rather diverse in the Parties at this point;
> - however, more harmonized rules for obtaining subscriber information would facilitate international cooperation.
>
> It is recommended that the T-CY:
>
> - facilitate greater harmonization between the Parties on the conditions, rules and procedures for obtaining subscriber information;
> - encourage Parties to take account of the observations of this report when reforming their domestic regulations.

# 3 Relevant court decisions and international developments

## 3.1 German Federal Constitutional Court (2012): Access to subscriber information under the Telecommunications Act

### 3.1.1 Summary

A decision of the German Federal Constitutional Court of 2012 offers valuable insights regarding the treatment of dynamic versus static IP addresses, including the question of proportionality. While it makes a distinction between subscriber information related to static versus dynamic IP addresses, it does not assimilate subscriber information for dynamic IP addresses with traffic data. It furthermore ruled that the general retention of subscriber information by service providers was constitutional.

In response to this decision, Germany developed a "double door" solution; the new provision 100j in the Criminal Procedure Code may serve as an example of good practice. Law enforcement can request the production of dynamic and static IP addresses, though for dynamic IP addresses there is an additional notification requirement which may be deferred or dispensed with under certain conditions.

Service providers now have a legal basis for disclosing data to law enforcement in the Telecommunication Act and law enforcement also have a legal basis for requesting subscriber information for static and dynamic IP addresses.

### 3.1.2 Decision 1 BVR 1299/05

The German Constitutional Court in January 2012 adopted decision (1 BVR 1299/05) on the constitutionality of Articles 111 to 113 of the Telecommunications Act (TKG). The TKG provides:

- in Article 111 that providers of telecommunication services must retain subscriber information from the beginning until one year after the end of the contract with a subscriber for the purposes of making these available under Articles 112 and 113 of the TKG;

- in Article 112 (procedure for automated access), that subscriber information must be made available for automated access by the German Network Agency (Bundesnetzagentur) which will make them available to courts, law enforcement services, customs, financial regulators, and security and intelligence services;

- in Article 113 (manual disclosure of data) that a telecommunication service provider is permitted to disclose subscriber information to authorities responsible for law enforcement, public safety as well as security and intelligence services. This includes IP addresses attributed at a specific moment in time and for this purpose the telecommunication provider may analyse traffic data. This provision also comprises the production of access codes (such as passwords, PINs or PUKs) used to protect access to end user devices or storage installations.

The Court decided that:

1. The attribution of telecommunication numbers to their users represented an interference with the right of informational self-determination (which is comprised under Article 2.1 (right to the free development of one's personality) in combination

with Article 1.1 (human dignity is inviolable) of the German Basic Law.[3] However, the attribution of dynamic IP addresses represented an interference with the fundamental right to the secrecy of communications of Article 10.1 of the German Basic Law.

In this respect, the Court considered that:

- Article 10.1 of the Basic Law protects the confidentiality of specific telecommunications events, it extends to the content of the communication but it does not extend to the totality of all information such as the attribution of the telecommunications numbers allocated by the service providers to particular subscribers. Article 10.1 of the Basic Law was also not affected if the attribution of a specific number to a subscriber permitted a public authority to reconstruct the content or circumstances of specific communications events and to attribute them to a specific person. This applies to static IP addresses in as the same way as to telephone numbers.

- This was different for dynamic IP addresses, but not because they are allocated for a specific communication but because a service provider needed to analyse traffic data to identify the subscriber of an IP address at a specific time. This is why the manual procedure of Article 13.1 TKG, with respect to dynamic IP addresses, interfered with the secrecy of communications as protected by Article 10.1 Basic Law.

The Court also noted that the manual procedure of Article 113 not only covered providers of public communication services but all those who commercially provide or contribute to such services, including providers of corporate or wireless networks in hospitals, hotels and others. In 2004, this may have comprised some 400,000 providers, while the obligation for automated access of Article 112 only covered a few hundred providers.

At the same time, according to information provided by the Government in this case, the automated procedure of Article 112 was used pre-dominantly in practice. In 2008/9, some 1,000 public authorities had issued 4.2 million requests for 26.6 million disclosures of data held by 120 service providers.

2. A separate legal basis was required for the transmission and the retrieval of data. It was not sufficient that the TGK permitted service providers to disclose subscriber information. Criminal justice and other authorities needed their own legal basis to request such data ("double door" solution).

3. The automated access procedure of Article 112 TKG, including the prior retention of subscriber information under Article 111 TKG, was in conformity with the Constitution (Basic Law).

   Data protection experts had argued that Article 111 TKG which provides for the retention of subscriber information by service providers violated the general prohibition of general data retention, while the Government argued that the retention of subscriber information under Article 111 was an interference of low intensity.

[3] The "Grundgesetz" (Basic Law) is the Constitution.

The Court ruled in this respect that:

- the retention of subscriber information under Article 111 TKG was constitutional. The data to be retained and thus the inference with rights was limited and proportionate;

- the purpose was to establish a reliable basis for making data available under Articles 112 and 113 TKG. The right of informational self-determination of Article 2.1 in combination with Article 1.1 of the Basic Law did not prohibit all types of retention of data but only required a higher threshold of necessity. As Article 111 TKG regulated the retention of limited and specifically defined data for a specifically defined purpose, this provision did not fall under the prohibition of data retention. The subscriber information to be retained did not allow drawing conclusions on the content or further context of communications. Moreover, static IP addresses were primarily allocated to institutional subscribers and less to individual users, and this limited the impact. This may change under IPv6;[4]

- this provision served as an appropriate means to achieve a specific purpose.

The Court also ruled that the automated procedure of Article 112 TKG was constitutional.

4. The manual procedure to access data of Article 113 TKG was in conformity with the Constitution if interpreted in line with the Constitution. However, the procedure of Articles 113.1 may not be used to attribute dynamic IP addresses.

5. The production of access codes can only be requested if the conditions for their actual subsequent use are given. In its present form it was not proportionate and thus was unconstitutional.

For reasons of public interest, the Constitutional Court did not declare the contentious provisions void but gave the legislator until 30 June 2013 to put in place new solutions.

### 3.1.3 Solutions

With respect to the question of subscriber information pertaining to both, static and dynamic IP addresses for the purpose of criminal investigations, the solution is a new Article 100.j of the German Criminal Procedure Code which now represents the first door of the "double door".

Article 100j says that if it is necessary to establish the facts or determine the location of an accused person, law enforcement and other criminal justice authorities may request the production of subscriber information available under Articles 95 and 111 TKG. This includes IP addresses attributed to a subscriber at a specific time (that is, dynamic IP addresses).

[4] See para 161 of *Order of 24 January 2012 - 1 BvR 1299/05*:
"However, § 112 TKG may acquire substantially greater weight of encroachment if static IP addresses in future – for example on the basis of Internet Protocol Version 6 – should become more widely used as the basis of internet communication. For the question of the weight of encroachment of the identification of an IP address does not primarily depend – even if a number of fundamental rights apply in this case – on whether an IP address is technically dynamic or static, but on the actual significance of the creation of a duty of information in this connection. But if in practice static IP addresses are allocated to a great extent to private persons too, this may possibly mean that the identities of internet users are broadly or at least largely determined and that communications events in the internet are de-anonymised not only for a limited period of time, but permanently. Such a far-reaching possibility of de-anonymisation of communication in the internet goes beyond the effect of a traditional telephone number register."

However, for dynamic IP addresses, the person concerned has to be notified if and when the purpose of the investigation is not put at risk. The person may not be notified if this is against protected interests of third persons or of the person concerned. If notification is deferred or dispensed with, this must be documented. Requests for the production of access codes (PUK, PIN or passwords for devices) require a court decision.[5]

## 3.2 Supreme Court of Canada (2014): Spencer

### 3.2.1 Summary

In the case of R. v.Spencer (2014 SCC 43), the Canadian police had "identified an Internet Protocol (IP) address of a computer that someone had been using to access and store child pornography through an Internet file-sharing program. They then obtained from the Internet Service Provider (ISP), without prior judicial authorization, the subscriber information associated with that IP address."

The Supreme Court of Canada considered that the "subject matter of the search was not simply a name and address of someone in a contractual relationship with the ISP. Rather, it was the identity of an Internet subscriber which correspond to particular Internet usage [Emphasis added]."

> "Subscriber information, by tending to link particular kinds of information to identifiable individuals, may implicate privacy interests relating to an individual's identity as the source, possessor or user of that information. Some degree of anonymity is a feature of much Internet activity and depending on the totality of the circumstances, anonymity may be the foundation of a privacy interest that engages constitutional protection against unreasonable search and seizure. In this case, the police request to link a given IP address to subscriber information was in effect a request to link a specific person to specific online activities [Emphasis added]. This sort of request engages the anonymity aspect of the informational privacy interest by attempting to link the suspect with anonymously undertaken online activities, activities which have been recognized in other circumstances as engaging significant privacy interests."

> "In the totality of the circumstances of this case, there is a reasonable expectation of privacy in the subscriber information. Therefore, the request by the police that the ISP voluntarily disclose such information amounts to a search."

The Court held that this search was unlawful.

Nevertheless:

> "The police, however, were acting by what they reasonably thought were lawful means to pursue an important law enforcement purpose. The nature of the police conduct in this case would not tend to bring the administration of justice into disrepute. While the impact of the Charter -infringing conduct on the Charter -protected interests of the accused weighs in favour of excluding the evidence, the offences here are serious. Society has a strong interest in the adjudication of the case and also in ensuring the justice system remains above reproach in its treatment of those charged with these serious offences. Balancing the three factors, the exclusion of the evidence rather than its admission would bring the administration of justice into disrepute. The admission of the evidence is therefore upheld."

[5] For an English version of the German Criminal Procedure Code see https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html#p0677 However, the translation is in parts misleading. For example, in the English version it is termed "Section 100j – Request for Information" while in the original German version it is termed "100j – Bestandsdatenauskunft", that is, "Provision of subscriber information".

### 3.2.2 Analysis and outcomes

Similarly to the finding of the German Constitutional Court that a separate legal basis was required, and that it was not sufficient that the law permitted disclosure, the SCC held that although the Canadian statute that governs commercial conduct in relation to privacy (*Personal Information Protection and Electronic Documents Act* - PIPEDA) permitted disclosure, a separate authority was needed to disclose the identity linked to the IP address that led to Mr. Spencer (it was his sister's account) given that it revealed intimate information about his activities on the Internet. The SCC directed that another authority, a reasonable law, was needed, and that this requirement could be met by having a warrant. However, the Court also stated that nothing in the decision diminished the existing common law authority of the police to obtain subscriber information in exigent circumstances (i.e., without additional authority in the form of a warrant or other reasonable law), and also held that subscriber information could be provided pursuant to a reasonable law or where there is no reasonable expectation of privacy.

In practice, following the SCC ruling in *R. v. Spencer*, and in the absence of any law designed specifically for access to subscriber information, the police have been obtaining court orders where possible, often seeking a general production order which can be used for any information, including to obtain subscriber information, when there are reasonable grounds to believe that an offence has been committed and that the information is in possession or control of the person being asked to provide it. However, this process has posed challenges for police. A key issue is that the threshold of "reasonable grounds to believe" is not always possible to meet in the early stages of an investigation, when subscriber information may be needed but where no such grounds yet exist.

These challenges for police were identified as part of a recent national public consultation in 2016 on national security. Many of those who responded to the consultation indicated their concerns with respect to privacy protections in relation to police access to subscriber information. Many respondents indicated that they considered this information to require a high level of privacy protection, and that it should require court orders prior to its being accessed. The principal area of concern in relation to privacy interests was the potential for links to be made between subscriber information and other information that could reveal other activities or location.[6] The legislation presented to Parliament on national security following this consultation (Bill C-59, National Security Act, 2017) did not contain any provisions relating to the issue of access to subscriber information.

## 3.3 Court of Justice of the European Union (2014 and 2016): Data retention decisions

The preliminary rulings of the European Court of Justice (CJEU) on data retention of 2014 and 2016 are not specifically about the question of subscriber information. They are nevertheless relevant because:

- EU Directive 2006/24/EC required the retention of a range of categories of data, including of IP addresses attributed to subscribers, and thus rules on access to subscriber information in EU Member States may be similar to those for accessing traffic data;

- the general retention of various categories of data "as a whole" is considered disproportionate. The retention of or access in specific criminal investigations to

[6] For more information consult the "National Security Consultations: What We Learned" Report, available on the Public Safety Canada website (www.publicsafety.gc.ca) with more detailed information on the responses to the consultations, and "Our Security, Our Rights, National Security Green Paper, 2016", under the theme "Investigative Capabilities in A Digital World" and the related Background Document, available on the same website, to see the text provided to the public on this issue to inform the consultation.

more limited categories of data such as subscriber information may not fall under the strict limitations set by the CJEU.

### 3.3.1 Directive 2006/24/EC on data retention

In 2006, the European Union adopted "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" (E-privacy Directive).

The E-privacy Directive 2002/58/EC provides in Article 15 that EU Member States may adopt data retention measures:

> Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period [emphasis added] justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

The aim of the Data Retention Directive was "to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law" (Article 1.1 Directive 2006/24/EC).

Article 1 also stated that the Directive "shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network."

Article 2 defined "data" as "traffic data and location data and the related data necessary to identify the subscriber or user".

Thus, a distinction is made between traffic data and subscriber information. However, the categories of data to be retained under Article 5 included subscriber information:

(a) data necessary to trace and identify the source of a communication:
  (1) concerning fixed network telephony and mobile telephony:
    (i) the calling telephone number;
    (ii) the name and address of the subscriber or registered user;
  (2) concerning Internet access, Internet e-mail and Internet telephony:
    (i) the user ID(s) allocated;
    (ii) the user ID and telephone number allocated to any communication entering the public telephone network;
    (iii) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;

In consequence, some EU Member States may treat traffic data and subscriber information in the same way when adopting national rules for the retention of data and access to such data.

### 3.3.2 Preliminary rulings of the CJEU (2014 and 2016)

**The Digital Rights Ireland decision (2014)**

The CJEU decided in 2014 that Directive 2006/24/EC on data retention was invalid, and in 2016 that any national legislation in EU Member States providing for the general and indiscriminate retention of all traffic and location data is precluded.

In the preliminary ruling on the joint cases C-293/12 Digital Rights Ireland and C-594/12 Seitlinger and others of 2014, the CJEU ruled that Directive 2006/24/EC on data retention was invalid.

The CJEU observes that:

> 26 … that the data which providers of publicly available electronic communications services or of public communications networks must retain, pursuant to Articles 3 and 5 of Directive 2006/24, include data necessary to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to identify the location of mobile communication equipment, data which consist, inter alia, of the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for Internet services. Those data make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.
>
> 27 Those data, taken as a whole [emphasis added], may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.

The CJEU agrees that while the Directive represents an interference with Articles 7 (Respect for private and family life) and 8 (Protection of personal data) of the Charter of Fundamental Rights of the European Union, it satisfied an objective of general interest:

> 43 In this respect, it is apparent from recital 7 in the preamble to Directive 2006/24 that, because of the significant growth in the possibilities afforded by electronic communications, the Justice and Home Affairs Council of 19 December 2002 concluded that data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention of offences and the fight against crime, in particular organised crime.
>
> 44 It must therefore be held that the retention of data for the purpose of allowing the competent national authorities to have possible access to those data, as required by Directive 2006/24, genuinely satisfies an objective of general interest.

When verifying the proportionality of the interference, the CJEU considers that "the retention of such data may be considered to be appropriate for attaining the objective pursued".

However, it notes the broad scope of the Directive (which "covers, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime", which interferes with the rights of "practically the entire European population") and concludes that this was not strictly necessary.

And while the aim of the Directive was to contribute to the fight against serious crime, there was no relation between the data to be retained and a threat to public security.

Furthermore, there was a general absence in the Directive of limitations to access to data retained by national authorities.

In conclusion:

> 69 Having regard to all the foregoing considerations, it must be held that, by adopting Directive 2006/24, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter.
>
> 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.

**The Tele2 Sverige and Watson decision (2016)**

The requests for a preliminary ruling in the joint cases C-203/15 Tele2 Sverige and C-698/15 Watson concerned the interpretation of Article 15(1) of the e-Privacy Directive 2002/58/EC and whether the preliminary ruling of the CJEU regarding Digital Rights Ireland of 2014 which had declared the Data Retention Directive invalid also affected the validity of any national legislation in EU Member States, specifically with regard to rules on access to retained data.

In its judgment (paragraph 99), the CJEU repeats the observation of the Digital Rights Ireland decision, namely that the "data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained…" and that the "data provides means … of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications."

The CJEU states that national legislation providing for the general retention of data "exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society…" (paragraph 107). The CJEU then refers to the possibility of Member States adopting measures for "targeted retention" of data:

> 108 However, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.

It is not clear what such "targeted retention" would mean in practice and whether it would be different from the real-time collection of traffic data foreseen in the Budapest Convention or measures carried out by national security and intelligence bodies.

The CJEU furthermore establishes strict criteria for access to data retained, limiting it to cases of serious crime and requiring judicial or other independent review.

The CJEU finally ruled:

> 1. Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.
>
> 2. Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union.

### 3.4 Constitutional Court of Portugal (2017): judgment no. 420/2017 on the retention of subscriber information

In its decision 420/2017 the Constitutional Court of Portugal in 2017 – while taking into account the CJEU's data retention decisions of 2014 and 2016 – declared the retention of subscriber information with respect to dynamic IP addresses as constitutional.

The decision concerned a case of child abuse materials where a request by a prosecutor for authorisation to transmit data to identify a user to whom an IP address had been assigned was rejected by the District Court of Lisbon in October 2016 on the grounds that Law 32/2008 on which the request was based was unconstitutional.

Law 32/2008 had transposed the EU Data Retention Directive 2006/24/EC into the domestic law of Portugal. This Directive was declared void by the CJEU in 2014.

While Law 32/2008 requires the retention all categories of data as listed in the former Directive, the Constitutional Court addressed the above issue only with respect to "source data", that is, "data relating to the name and address of the subscriber or registered user to whom an IP address was assigned at the time of the communication, in accordance with Article 6 and Article 4(1)(a)(2), and no. 2(b)(iii), both of Law no. 32/2008 of 17 July".

The Constitutional Court of Portugal took into account the CJEU decisions of 2014 (Digital Rights Ireland) and 2016 (Tele2 Sverige) and concluded that:

- "The Court of Justice does not have the jurisdiction to assess the validity of the acts of national law of the Member States, since its analysis only focuses on the text of

the directive. The validity of Law no. 32/2008, of 17 July, cannot be called into question simply because this EU regulatory act has been declared invalid."

- Portugal, when transposing the Data Retention Directive, introduced an extensive and complex framework, including on access to and protection of retained data.[7]

- "Since national solutions differ from EU standards, a judgement on their constitutionality must take account of these differences."

The Court decided that these provisions requiring service providers to retain "source data" (that is, subscriber information related also to dynamic IP addresses) for a period of one year was constitutional.

## 3.5 European Court of Human Rights (2018): Benedik versus Slovenia

### 3.5.1 Summary

The case of Benedik versus Slovenia is the first decision of the ECtHR dealing with the nature of IP addresses.

The ECtHR found a violation of Article 8 of the European Convention of Human Rights primarily because the relevant law, and its application in the concrete case, on access to subscriber information associated with a dynamic IP address lacked clarity and because of the reasoning of the Slovenian Constitutional Court that in the concrete case Mr. Igor Benedek had waived his expectation of privacy.

The Constitutional Court – contrary to lower courts in Slovenia – had held that the subscriber information related to dynamic IP addresses requested by the police in this case was part of a concrete communication which in principle is protected by the Slovenian Constitution and for which, therefore, a court order would have been required. Article 149b(1) of the Criminal Procedure Code required a court order for traffic data (including on participants and other circumstances of the communication), while subscriber information related to the means of communication could have been requested by the police without court order under Article 149b(3) CPC.

The Constitutional Court decided that while a court order would have been required, in the concrete case Mr. Igor Benedik had waived his expectation of privacy when downloading and sharing child abuse materials in a peer-to-peer network, and that thus the procedure of the police to obtain the subscriber information from a service provider without a court order was lawful.

[7] "… when transposing the Directive into national law, the Portuguese legislator (i) established rules for data access, subject to the criteria of necessity, suitability and proportionality, to be verified also with respect to the definition of data categories (Article 9(1) and (4)) and limiting it to a restricted listing of the data subjects (Article 9(3)); (ii) defined the concept of serious crimes (Article 2(1)(g); (iii) imposed the precedence of court orders on data access, upon request of the Public Prosecutor or the appropriate criminal police authority (Article 9(2)); (iv) established specific duties on the protection and security of data, including creating a computer application called "system for data access or request for communications carriers" (SAPDOC), from which there is a process for communicating and accessing data through a secure link, encrypted by user name and password, through the requirement for electronically recording the requests for data sent, including an indication of who made the submission, and the date and time at which the same occurred, as well as access to the response files, also with an indication of who did so, and the date and time of each access (Article 7(3) of Law no. 32/2008 and Decree no. 469/2009); and (v) made express provision for the judicial decision to transmit the data to duly preserve professional secrecy under the law, although not to avoid their retention (Article 9(4)). (...)" [Informal translation of the Court decision]

### 3.5.2 The decision of the ECtHR

In this case, the Slovenian police had received information in 2006 on an IP address used in a file sharing network for child abuse materials from the Swiss authorities. The Slovenian police then obtained subscriber information related to this dynamic IP address from a Slovenian service provider under Section 149b(3) of the Criminal Procedure Act which required service providers to disclose subscriber information without a court order:[8]

> Section 149b(3) If there are grounds for suspecting that a criminal offence for which a perpetrator is prosecuted *ex officio* has been committed or is being prepared, and information on the owner or user of a certain means [emphasis added] of electronic communication whose details are not available in the relevant directory, as well as information on the time that the means of communication was or is in use, needs to be obtained in order to uncover this criminal offence or the perpetrator thereof, the police may request that the operator of the electronic communications network furnish them with this information, at their written request and even without the consent of the individual to whom the information refers.

In a second step, the police via a prosecutor obtained a court order for the production of further subscriber and traffic data linked to the IP address, and in a third step, another court order to search the house of the subscriber. Child pornography (images and videos) and software to download and share such materials were then found on the computer of the son of the owner, Mr. Igor Benedik (the applicant).

The Kranj District Court subsequently convicted the applicant to a suspended prison term of 8 months. The Ljubljana Higher Court rejected an appeal and held that the information on the user of the IP address had been obtained lawfully and that no court order was required.

The applicant lodged a further appeal reiterating that a dynamic IP address should be considered traffic data and that it was, therefore, obtained unlawfully by the police in the first place. The Supreme Court rejected the appeal on the grounds that the police had not acquired traffic data "but only data regarding the user of a particular computer through which the Internet had been accessed".

The case then went to the Slovenian Constitutional Court which in 2014 – contrary to the previous courts –considered that Article 37 of the Constitution protected traffic data and that IP addresses were included in such traffic data.

It concluded, however, that:

> the applicant, who had not hidden in any way the IP address through which he had accessed the Internet, had consciously exposed himself to the public and could not legitimately have expected privacy. As a result, the data concerning the identity of the user of the IP address were not protected as communication privacy under Article 37 of the Constitution, but only as information privacy under Article 38 of the Constitution, and no court order was required in order to disclose them in the applicant's case.[9]

Mr. Benedik then submitted his application to the European Court of Human Rights, referring, among other things, to the decision of the German Federal Constitutional Court of 2012.

[8] Section 149b(1) in contrast requires a court order in case the information is related to a communication and not the means:
"(1) If there are grounds for suspecting that a criminal offence for which a perpetrator is prosecuted ex officio has been committed, is being committed or is being prepared or organised, and information on communications using electronic communications networks needs to be obtained in order to uncover this criminal offence or the perpetrator thereof, the investigating judge may …."

[9] Quoted from Paragraph 28 of the decision by the ECtHR.

In the ECtHR's assessment:

- "an IP address is a unique number assigned to every device on a network, which allows the devices to communicate with each other. Unlike the static IP address, which is permanently allocated to a particular network interface of a particular device, a dynamic IP address is assigned to a device by the ISP temporarily, typically each time the device connects to the Internet"[10] and that to obtain the name and address of the subscriber using a dynamic IP address, the ISP is normally required to look up this information and for that purpose to examine the relevant connection data of its subscribers";[11]

- personal information on telephone, email and Internet usage fall within the ambit of Article 8 of the European Convention of Human Rights as considered by the ECtHR in previous cases;[12]

- "the subscriber information associated with specific dynamic IP addresses assigned at certain times was not publicly available and therefore could not be compared to the information found in the traditional telephone directory or public database of vehicle registration numbers referred to by the Government … Indeed, it would appear that in order to identify a subscriber to whom a particular dynamic IP address had been assigned at a particular time, the ISP must access stored data concerning particular telecommunication events";[13]

In its judgment, the ECtHR reviewed comparative law, including the German Constitutional Court[14] and the Supreme Court of Canada decisions mentioned above,[15] and adopted a contextual approach.

It underlined that the subscriber information was linked to specific content shared by an individual:

> 109. Furthermore, the Court cannot ignore the particular context in which the subscriber information was sought in the present case. The sole purpose of obtaining the subscriber information was to identify a particular person behind the independently collected content revealing data he had been sharing. The Court notes in this connection that there is a zone of interaction of a person with others which may fall within the scope of "private life" (see paragraph 100 above). Information on such activities engages the privacy aspect the moment it is linked to or attributed to an identified or identifiable individual (for reference to identifiability, albeit in a rather different context, see *Peck v. the United Kingdom*, no. 44647/98, § 62, ECHR 2003-I, and *J.S. v. the United Kingdom* (dec.), no. 445/10, §§ 70 and 72, 3 March 2015). Therefore what would appear to be peripheral information sought by the police, namely the name and address of a subscriber, must in situations such as the present one be treated as inextricably connected to the relevant pre-existing content revealing data (see the dissenting Constitutional Court judges' opinions cited in paragraphs 31 and 34; compare also with the position of the Canadian Supreme Court, cited in paragraphs 69 and 72 above, and the German Federal Constitutional Court, cited in paragraphs 64 and 65 above). To hold otherwise would be to deny the necessary protection to information which might

[10] Comment: This does not appear to be correct. A dynamic IP address is not assigned for each new communication but may be assigned for a considerable period of time. A dynamic IP address is thus not necessarily linked to a concrete communication.
[11] Paragraph 96 of Benedik v. Slovenia.
[12] Paragraph 104 of Benedik v. Slovenia.
[13] Paragraph 108 of Benedik v. Slovenia.
[14] Paragraphs 63-67 of Benedik v. Slovenia.
[15] Paragraphs 68-72 of Benedik v. Slovenia.

> reveal a good deal about the online activity of an individual, including sensitive details of his or her interests, beliefs and intimate lifestyle.[16]

The ECtHR further noted that:

> … section 149b(3) of the CPA (see paragraph 36 above), relied on by the domestic authorities, concerned a request for information on the owner or user of a certain means of electronic communication. It did not contain specific rules as to the association between the dynamic IP address and subscriber information. The Court further notes that Article 37 of the Constitution required a court order for any interference with privacy of communication… Furthermore, the ECA … which specifically regulated the secrecy and confidentiality of electronic communication, did not at the relevant time provide for the possibility that subscriber information and related traffic data be accessed and transferred for the purposes of criminal proceedings.[17]

The ECtHR referred to Article 15 Budapest Convention, however, without elaborating on the notion of "as appropriate":

> 126. Having regard to the particular context of the case, the Court would emphasise that the Cybercrime Convention obliges the States to make measures such as the real-time collection of traffic data and the issuing of production orders available to the authorities in combating, *inter alia*, crimes related to child pornography (see paragraphs 47 to 51 above). However, such measures are, pursuant to Article 15 of that Convention, "subject to conditions and safeguards provided for under [State parties'] domestic law" and must "as appropriate in view of the nature of the procedure or power concerned, *inter alia*, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure …"

The ECtHR then observed in particular that:

> … the only reason for the Constitutional Court dismissing the applicant's complaint – that is, for approving of the disclosure of the subscriber information without a court order – was the presumption that the applicant had "waived the legitimate expectation of privacy" (see paragraph 18 of the Constitutional Court's decision, cited in paragraph 29 above). However, the Court, having regard to its findings in the context of the applicability of Article 8, does not find the Constitutional Court's position on that question to be reconcilable with the scope of the right to privacy under the Convention (see paragraphs 115 to 118 above). Bearing in mind the Constitutional Court's finding that the "identity of the communicating individual" fell within the scope of the protection of Article 37 of the Constitution (see paragraph 128 above) and the Court's conclusion that the applicant had a reasonable expectation that his identity with respect to his online activity would remain private (see paragraphs 115 to 118 above), a court order was necessary in the present case.[18]

The ECtHR, therefore, held that there had been a violation of Article 8 of the European Convention of Human Rights.

As a consequence of this case and of the earlier Slovenian Constitutional Court decision, the practice changed, and Slovenian law enforcement now seek a court order for static and

[16] Comment: This statement by the ECtHR raises questions: Isn't it always the case that whenever law enforcement asks for subscriber information, be it in relation to dynamic or static IP addresses or simple telephone or vehicle numbers, the purpose is to link a number and thus a subscriber to a specific criminal event, including content?

[17] Paragraph 127 of Benedik v. Slovenia.
[18] Paragraph 128 of Benedik v. Slovenia.

dynamic IP addresses in relation to concrete communications. Amendments to the Criminal Procedure Code are still pending.

### 3.6 Court of Justice of the European Union (2018): Case C-207/16 Ministerio Fiscal

The request for a preliminary ruling in case C-207/16 concerned the question of whether access to subscriber information – here to identify users of telephone numbers activated with a stolen telephone – must be restricted to serious crime. The CJEU decided in October 2018 that access to subscriber information "cannot be defined as 'serious' interference with the fundamental rights of persons" and that access thus may not be limited to cases of serious crime.

In the case in question,

> In the context of an investigation into the robbery of a wallet and mobile telephone, Spanish police requested the investigating magistrate in charge of the case to grant them access to data identifying the users of telephone numbers activated with the stolen telephone during a period of 12 days as from the date of the robbery. The investigating magistrate rejected the request on the ground, inter alia, that the acts giving rise to the criminal investigation did not constitute a 'serious' offence — that is, an offence punishable under Spanish law by a term of imprisonment of more than five years –, access to identification data being possible only in respect of that category of offences. The Ministerio Fiscal (Spanish Public Prosecutor's Office) appealed against that decision before the Audiencia Provincial de Tarragona (Provincial Court, Tarragona, Spain).[19]

As in the CJEU decisions on data retention discussed above, Case C-207/16 concerned an interpretation of Article 15(1) of the E-privacy Directive 2002/58/EC in relation to other European Union law. And while this case concerned access to data retained under Spanish data retention legislation, the CJEU did not seek to examine the validity of data retention regulations in this preliminary ruling but only the question of access to such data by public authorities.

According to the decision of the CJEU:

> 60 It is therefore apparent that the data concerned by the request for access at issue in the main proceedings only enables the SIM card or cards activated with the stolen mobile telephone to be linked, during a specific period, with the identity of the owners of those SIM cards. Without those data being cross-referenced with the data pertaining to the communications with those SIM cards and the location data, those data do not make it possible to ascertain the date, time, duration and recipients of the communications made with the SIM card or cards in question, nor the locations where those communications took place or the frequency of those communications with specific people during a given period. Those data do not therefore allow precise conclusions to be drawn concerning the private lives of the persons whose data is concerned.
>
> 61 In those circumstances, access to only the data referred to in the request at issue in the main proceedings cannot be defined as 'serious' interference with the fundamental rights of the persons whose data is concerned.
>
> 62 As stated in paragraphs 53 to 57 of this judgment, the interference that access to such data entails is therefore capable of being justified by the objective, to which the first sentence of Article 15(1) of Directive 2002/58 refers, of preventing, investigating, detecting and

[19] Quoted from the Press Release published on 2 October 2018.

> prosecuting 'criminal offences' generally, without it being necessary that those offences be defined as 'serious'.
>
> 63 In the light of the foregoing considerations, the answer to the questions referred is that Article 15(1) of Directive 2002/58, read in the light of Articles 7 and 8 of the Charter, must be interpreted as meaning that the access of public authorities to data for the purpose of identifying the owners of SIM cards activated with a stolen mobile telephone, such as the surnames, forenames and, if need be, addresses of the owners, entails interference with their fundamental rights, enshrined in those articles of the Charter, which is not sufficiently serious to entail that access being limited, in the area of prevention, investigation, detection and prosecution of criminal offences, to the objective of fighting serious crime.

In short, and relating this case to the present study, the CJEU decided that:

- subscriber information does "not allow precise conclusions to be drawn concerning the private lives of the persons whose data is concerned";
- therefore, access to subscriber information "cannot be defined as 'serious' interference with the fundamental rights of the persons whose data is concerned",
- thus while access to subscriber information of users "entails interference with their fundamental rights [… ] which is not sufficiently serious to entail that access being limited, in the area of prevention, investigation, detection and prosecution of criminal offences, to the objective of fighting serious crime."

## 3.7 EU draft Regulation on European Production and Preservation Orders

On 17 April 2018, the European Commission published a proposal for a regulation on European Production and Preservation Orders for electronic evidence in criminal matters.

The draft Regulation is to permit criminal justice authorities of EU Member States to send production orders for data to a service provider offering a service in one Member State that is based in another Member State. A complementary draft Directive requires service providers offering services within the EU to have a legal representative in at least one EU Member States to which a request could be sent.

A difference is made between requests for "transactional data" (similar to traffic data) and content data on the one hand, and subscriber information and a new category of "access data" on the other: a production order for content and transactional data is to be issued or to be validated by a judge, while a production order for subscriber information and access data may be issued or validated by a prosecutor.

According to Article 2 (8):

> 'access data' means data related to the commencement and termination of a user access session to a service, which is strictly necessary for the sole purpose of identifying the user of the service, such as the date and time of use, or the log-in to and log-off from the service, together with the IP address allocated by the internet access service provider to the user of a service, data identifying the interface used and the user ID. This includes electronic communications metadata as defined in point (g) of Article 4(3) of [Regulation concerning the respect for private life and the protection of personal data in electronic communications];

According to the Explanatory Memorandum:

> It is appropriate to single out access data as a specific data category used in this Regulation. Access data as defined here is pursued for the same objective as subscriber data, i.e. to identify the user, and the level of interference with fundamental rights is similar. It should therefore be subject to the same conditions as subscriber data. Hence this proposal introduces a new category of data, which is to be treated like subscriber data if the same aim is pursued.

The inclusion of metadata as defined by the future "Regulation concerning the respect for private life and the protection of personal data in electronic communications" may lead to a confusion of "access data" with the type of traffic (or meta) data for which a higher threshold is often required following decisions of the CJEU and a number of domestic constitutional courts of EU Member States. According to point (c)[20] of Article 4(3) this draft Regulation:

> (c) 'electronic communications metadata' means data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication;

# 4 Considerations

This brief review of domestic and international court decisions and developments regarding subscriber information leads to some theses for further consideration:

1. The purpose of obtaining subscriber information in a criminal justice context – be it in relation to static or dynamic IP addresses (or telephone numbers for that matter) – is the same, namely, to identify the subscriber of a specific account or website, or the subscriber of an IP address in relation to a specific criminal investigation. Obtaining subscriber information thus permits investigating authorities inter alia to reconstruct the link between a subscriber and a concrete communication, or vice versa. However, subscriber information as such does not permit precise conclusions to be drawn in respect of the private lives of individuals. The retention and production of subscriber information as such is unlikely to interfere with the right to the secrecy of communications, although it is likely to interfere with other rights.

2. The disclosure of subscriber information in specific criminal investigations, in principle, represents a less serious interference with the rights of individuals, including rights to the secrecy of communication or to informational self-determination, than the disclosure of traffic or content data. Some Parties or their courts, therefore, consider it proportionate to foresee lower thresholds for the disclosure of subscriber information than for traffic or content data. In some other States, jurisprudence suggests that these issues must be addressed contextually and that the disclosure of subscriber information may attract a higher level of privacy interests in a given context and that a case by case assessment would thus be necessary.

3. Criminal justice authorities may require access to subscriber information in specific criminal investigations below the threshold of "serious crime". Limiting access to or disclosure of subscriber information to investigations of serious crime would prevent governments from meeting their obligations to protect individuals and their rights against crime as in the case of K.U. v. Finland of the ECtHR. Moreover, at the initial

[20] There seems to be a mistake in the draft Regulation: the correct reference should be point (c) of Article 4(3).

stage of an investigation the "seriousness" of the offences involved is often not yet obvious.

4. Subscriber information may comprise access numbers, including Internet Protocol addresses, strictly needed to identify a subscriber, such as the first login IP, last login IP or the login IP used at a specific moment in time.[21] This may need to be clarified in the 2nd Additional Protocol or its Explanatory Report. Introducing new categories of data, such as "access data", may lead to further misunderstandings regarding applicable rules on the retention of or access to such data and may be difficult to apply by practitioners.

5. State Parties may consider in their domestic legislation a legal requirement for the retention of subscriber information so as to be available for the purposes of specific criminal investigations. Several court decisions suggest that such measures may be appropriate and proportionate when it involves the retention of a limited set of data that does not allow conclusions to be drawn about the content of communications or the everyday habits or social relationships of an individual.

6. Some jurisprudence and domestic rules distinguish between static and dynamic IP addresses assigned to a specific subscriber and consider the production of subscriber information related to dynamic IP addresses as being an interference with the right to the secrecy of communications. Further discussions are needed in this respect:

   - On the one hand, the argument that a dynamic – as opposed to a static – IP address is always linked to a concrete communication is not accurate:

     - A dynamic IP address may be assigned to a subscriber for days or months or until a router reset, for example.
     - The device of a user may auto-connect to the Internet without the active involvement or without an actual communication of the individual.
     - For static IP addresses or telephone numbers as well, the intended result of an investigation is to link a subscriber to a concrete communication or event.

   - On the other hand, service providers may need to analyse or look up traffic data to determine the IP address assigned to a subscriber at a specific point in time. Even if the service provider does not disclose such related traffic data to the criminal justice authority and even if this analysis or look-up does not represent an analysis of the content or context of a communication and does not permit to draw precise conclusions in respect to the private life of a person, such an analysis or look-up by the service provider is not needed for static IP addresses. However, the seriousness of impact of such an analysis or look up on the privacy or other rights of individuals is arguable given that such a look up as well as is likely to entail an automated query of databases.

7. Access to subscriber information, in relation to both static and dynamic IP addresses, requires a legal basis, such as implementation of the production orders of Article 18 Budapest Convention in domestic law.[22] Such a specific provision on production orders would also clarify that this measure is different from and requires

[21] See the annex to the Template for MLA for subscriber information adopted by the T-CY in July 2018.
[22] Full implementation of Article 18 in domestic law was also recommended by the T-CY Cloud Evidence Group in its final report, the Recommendations of which were adopted by the T-CY in November 2016.

a lower threshold than search and seizure powers. The legal basis may be strengthened by specifically referring to or including IP addresses assigned at a specific time, that is, dynamic IP addresses. A "double door" regulation or other legislative measures (1) permitting a service provider to disclose such data, for example in a telecommunication law, and (2) a provision on production orders for both types of subscriber information establishing the conditions for criminal justice authorities to request such information, may, in combination, offer stronger safeguards and legal certainty.